When data is the new oil, it is our role to prevent the blowout!



Marc-Oliver Pahl, IMT Atlantique Rennes

Chair holder Chaire Cyber CNI Co-Directeur Equipe IRIS / UMR LAB-Sticc Digital Teaching Coordinator German-French Academy for the Industry of the Future chairecyber-cni.orgi Leader of the Smart Space Orchestration Team at TUM Vice President German Chapter of the ACM











Summer School AI 4 Industry Keynote, 2020-07-30, 9h00

Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)







- Part I: Motivation
- Part II: Security in the Wild
- Part III: Where to use AI?



Structure

My goal:

Encourage you to always consider security when creating algorithms, software, or products.

The onogoing digitization in all areas of life requires it - from each one of us!



Cybersecurity of Critical Infrastructures



Some Methods MACHINE and **Block**chain























CONTRACTOR OF



Mitigate

Self-Defend Security Incidents Self-Recover from Security Incidents

> Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)



CHAIRE

CYBER CNI

curité des infrastructures critiques

EST. 2016

	ରାଜ(ଉାଉ(ଉାଉ(ଉାଉ)ର ଭାଜ(ଉାଉ(ଉାଉ(ଉାଉ)ର	ත්ත්ත්තික කරන කරන කරන කරන කරන කරන කරන කරන කරන කර	ାରାରାରାରାରାରାରାରା ଅବନେକାରାରାରାରାରାରାରାରାରା ଅବନେକାରାରାରାରାରା ଅବନେକାରାରାରାରାରାରାରାରାରାରାରାରାରାରାରାରାରାରାର	a \@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@	000	~(@@@@@@@ @@@@@@@ @@@@@@@@	a a Na/a/a/a/a/a/a/a/a Na/a/a/a/a/a/a/a/a/a/	10/0/0/0/0/0/0/0/0/0/0/0/0/0/0/0/0/0/0/	-Va
	രരത്തിന്നത്തിന്ന	100 (00000 0000000	ଜଉଇଉଇଉଉଇଉଇଣ କାର୍ବରେଜିବିନ୍ଦ୍ର ଜେଉଭାର		ത്രമാരത്തരം	Dalalaa . a	<u>ର</u> ଜ୍ଞାନ୍ତର୍ଭୁ ଜୁନ୍ତର	1000000	
	രരരരരരര	V#@@@@@@@@@@@/@ @@				aaaaa a/	ର ଜାନ୍ତି ଜାନ୍ତି	u#aa a aa	@@(@&@@#wwww
	ଭାଜାରା ଭାରଣ କାର୍ଯ୍ୟ କାର ଭାରଣ କାର୍ଯ୍ୟ କାର	ରେଉଇ) ଇଉଇଉଇ (ଉଉଇଛରେ (ଉଉଇ	000000000000000000000000000000000000000	agaa . agaa . agaa	ର ଇଇଇଇଇଇଇ ଜ	aaaaa a/(a @, @@		@@@&(@@@%@@
	@@@@@@@@@@@@.	േര്ത്തിന്നെത്തിന്ന	മത്രത്തിന്റെ	<u>ଧ୍</u> ୟତାରାରା ସାହାରାରାରା ସାହାରା ସାହାରା ସାହାରା ସାହାରା ସାହାର ସ		100000000000000000000000000000000000000	a 1000a (0.000	രുരുരുത	aa
	<u>ର୍ଜ୍ ରାଜ୍ ଜାନ୍ତର୍ ରାଜ୍ ରାଜ୍</u> ୟ କାର୍ଯ୍ୟ	alanum Dalaalaa	alanananananananan Dahalalalahala	10,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,				Malalala Malalala	aa
Excession Excession <t< td=""><td>୶ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼</td><td>ରାର୍ଭଭାଭଭାଭାଇ କାର୍ଯ୍ୟ କ</td><td>ର୍ଭ୍ୟର୍ଭ୍ କ୍ରେକ୍ର୍ କ୍ରେକ୍ (ଜ୍ୟୁ କ୍ରେକ୍ର୍ କ୍ରେକ୍ର୍ କ୍ରେକ୍ର୍ କ୍ର୍ କ୍ର୍ କ୍</td><td>ରଜ୍ଜ୍ଭ୍ଭ୍ର୍</td><td>0.0000000000000000000000000000000000000</td><td>v@@@@@(</td><td>a)@@@@@@@</td><td>)@@@@@</td><td>രതരതരതര</td></t<>	୶ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼	ରାର୍ଭଭାଭଭାଭାଇ କାର୍ଯ୍ୟ କ	ର୍ଭ୍ୟର୍ଭ୍ କ୍ରେକ୍ର୍ କ୍ରେକ୍ (ଜ୍ୟୁ କ୍ରେକ୍ର୍ କ୍ରେକ୍ର୍ କ୍ରେକ୍ର୍ କ୍ର୍ କ୍ର୍ କ୍	ରଜ୍ଜ୍ଭ୍ଭ୍ର୍	0.0000000000000000000000000000000000000	v@@@@@(a)@@@@@@@)@@@@@	രതരതരതര
image: i	രരത്തിനുമായ	ാരത്രമരുതരുത്തും	ଗ୍ରାର୍ଭରାଗ୍ରାର୍ଗ୍ର ସେହି ଅନ୍ତ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍ମ୍ କ୍ରାର୍ମ୍ କ୍ରାର୍ମ୍ କ୍ରାର୍ମ୍ କ୍ରାର୍ମ୍ କ୍ରାର୍ମ୍ କ୍ରାର୍ମ୍ କ୍ରାର୍ମ ଭାରଣ କ୍ରାର୍ମ୍ କ୍ରାର୍ମ	<i>ଉ</i> (ଉ(ଉ)(ଉ)(ଉ)	0.0000000000000000000000000000000000000	0,	ര നമ്പരിയത്തിന്	Valaciaa Valaciaa	രരരരരരം
$ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\$	ଉତ୍ତାର୍ଭ୍ ଭାର୍ତ୍ତର କୁ	**8,0,.0,0,00 **#%%	(a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.	*###########	## ####################################	##*(//, ####@@@	1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	10000000	(ର୍ଗ୍ ର୍ଗ୍ ର୍ଗ୍ ର୍
000000000000000000000000000000000000	<u></u>	/ #/* ,	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	a@####@####)## # (/ , ##	#,.,* ###@@@	ര്ത്തത്തത്തെന്ന	<u>ക്കത്തത്തിന് പ്രത്തത്തിന് പ്രത്തത്തിന് പ്രത്തത്തിന് പ്രത്തത്തിന് പ്രത്തത്തിന് പ്രത്തത്തിന് പ്രത്തത്തിന് പ്രത്ത</u>	A
senders and set of the	0@@@@@@@@,*,~	er		+#%#&#&#%###</td><td>#+</td><td></td><td>a</td><td></td><td>(a)a)a(a)</td></tr><tr><td>000000000000000000000000000000000000</td><td>@@@@@@@@@, , , * . , #</td><td>#((%%@@@&##(#@&,.*/*/,/.***,6</td><td>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</td><td>#(, , ,/.##</td><td>#.,,,,,/#**.,,,(## #</td><td>,##/##,## (.##@@@</td><td>a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.a.</td><td>୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶</td><td>രരംഗരംഗരംഗരംഗം</td></tr><tr><td>modelessed </td><td>@@@@@@@@,,,/,(</td><td>(*//(#@%%###8&#,**(/*.*,/@</td><td>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</td><td>***********************</td><td>******************</td><td>.########################@@@@</td><td>aaaaaaaaaaaaaaaaaaaaaa, . , * , ,</td><td>**,,,,,,,,,,+++</td><td><u> (@@@</u>)</td></tr><tr><td><pre>mmmembers */, *, *, *, *, *, *, *, *, *, *, *, *, *,</td><td>alalalalala,,,/</td><td>/,(&/(,**,/,,&@&@@@#*(,/*@</td><td>ର୍ଗ୍ର ଭାଇତ୍ର ଭାଇତ୍ର ସ୍ଥାରେ କାର୍ଯ୍ୟ କାର୍</td><td><u>ଅଭାନ୍ତା</u>ର୍ବରାନ୍ତାର୍ବରାନ୍ତ୍ରରାନ୍ତ୍ରରାନ୍ତ୍ରରାନ୍ତ୍ରରାନ୍ତ୍ରରାନ୍ତ୍ର</td><td>ା<u>ଜ</u>ଭଭାଭଭାଇର୍ଭ୍ କ୍ରେର୍ଭ୍ କ୍ରେର୍ଭ୍ କ୍ରେର୍ଭ୍ କ୍ରେର୍ଭ୍ କ୍ରେର୍ଭ୍ କ୍ରେର୍ କ୍ରେର୍ କ୍ରେର୍ କ୍ରେର୍ କ୍ରେର୍ କ୍ରେର୍ କ୍ରେର୍ କ୍ର</td><td>0,</td><td>aaaaaaaaaaaaaaaaaaaaaaaaaaaa</td><td></td><td>, രരദ</td></tr><tr><td>production </td><td>@@@@@@@@@.*/,#</td><td>#(,*((* ,*/&%@*@/@&@/(#(@</td><td>୶୶ଢ଼</td><td>100000000000000000000000000000000000000</td><td>, %%##((%@@@@@@@@@@@@@@</td><td>ାର୍ଭଭାଜାଭାଇର୍ଭ୍ ରାହ୍ରର୍ଭ୍ ରାହ୍ରର୍ଭ୍ ରାହ୍ରର୍</td><td>ବ୍ୟର୍ଭର୍ଭ୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର</td><td>. ر * در / ر ر</td><td>/(</td></tr><tr><td>000000000000000000000000000000000000</td><td>/</td><td>,** .& * @%.&&&#%%@/@##(***@</td><td>ର୍ଗ୍ର ଭାଇନ୍ସ ସ୍ଥାରେ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ</td><td>aaaaaaaaaaaaaaa%##*</td><td>.,%@%%%#(%@@@@@@@@@@@@@</td><td>ରେଜାନ୍ତିର ଜଣ୍ଡରାଜନ୍ତି କରିହାନ୍ତି କରିହାନ୍ତି କରିହାନ୍ତି କରିହାର ଭାଇ ଭାଇ ଭାଇ ଭାଇ ଭାଇ ଭାଇ ଭାଇ ଭାଇ ଭାଇ ଭାଇ</td><td>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</td><td>المعوودون وور</td><td>., *.**.</td></tr><tr><td>0:00000000000000000000000000000000000</td><td>ର୍ଜ୍ଜ୍ ଜ୍ଜ୍ ନ୍ର୍ ((/ / /</td><td>//#& *.((*/,//(//0</td><td>ର୍ଗ୍ର ଅଭିନ୍ତି କ୍ରେମ୍ବର କ୍ରେମ୍ବ ଅଭିନ୍ତି କ୍ରେମ୍ବର କ୍ରେମ</td><td>3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0</td><td>%&/%#@##/@@@@@@@@@@@@@@@</td><td>ର୍ଭାରାରାରା ଭାରଣ କାର୍ଯ୍ୟରା କାର୍ଯ୍ୟ କାର୍</td><td><u>କରାରାରାରାରାରାରାରାରାରା</u></td><td>. /./**.,</td><td>*/*/(((#(.*</td></tr><tr><td>Conservation Conservation Conservation Conservation Conservation Conservation Conservation Conservation Conservation Conservation Conservation Conservation Conse</td><td>ରାଜାରାଜାରାଜାରାଜାରାଜାରାଜାରାଜାରାଜାରାଜାରାଜ</td><td>ର୍ବ୍ଦର୍ଭ ଭୁନ୍ତର୍ଭ୍ କୁହ୍ମର୍ଭ୍ କୁହ୍ମର୍</td><td>୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶</td><td>30000000000008% ,/&,</td><td>*%%% (% (@%@@@@@@@@@@@@@@@</td><td>##############</td><td>((((((((##@@@@@@</td><td></td><td>,&&&%%#(,</td></tr><tr><td>separatemanagement ////////////////////////////////////</td><td><u>ଜ୍ଞାର୍ଗ୍ର ଜ୍ଞାର୍</u>ଶ୍ୱର୍ଭ୍ କ୍ରାର୍ଗ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍ଗ୍ର କ୍ରାର୍</td><td>@@@@@@%*****************</td><td>********************************</td><td>*******@@@@@@@&/ ., *</td><td>,,*(%#*#(%@@@@@@@@@@@@@</td><td>muununun</td><td>((((((((((()</td><td></td><td>(%(,,</td></tr><tr><td>webselectoreset ////// ///// ///// ///// webselectoreset ///// ///// ///// ///// webselectoreset ///// ///// ///// ///// webselectoreset ///// ///// ///// ///// ///// webselectoreset ///// /// <td</td><td>0@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@</td><td>000000%*********************</td><td>** * ,* * * ,,*****************</td><td>*******@@@@@@&%&(,,,</td><td>*&&&%#,%@@@@@@@@@@@@@</td><td>(#(##%(#%**#(/((///</td><td>//(((((((@@@@@@</td><td>- 1</td><td>#(*//*,</td></tr><tr><td>biological concept conc</td><td>൭൏൏൏൏൏൏൏൏൏൏</td><td>000000%********************************</td><td>** /* , */*/ *,/,*********</td><td>*******@@@@@@(* ,.(#(</td><td>###%%##, #@@@@@@@@@@@@@@</td><td>////*(/**//*/%#,.(#</td><td>./,*******@@@@@@,</td><td>., ////.#,*, *</td><td>@(*,/</td></tr><tr><td>processor Construction Co</td><td>000000000000000000000000000000000000000</td><td>000000%*******************</td><td>******</td><td>*******@@@@@@@% **</td><td>*//(((/#@@@@@@@@@@@@@@</td><td>/,,,*#/**/,&,* //</td><td>/,*******</td><td><u>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</u></td><td>#8%&/@@@@&&</td></tr><tr><td>Decempoint State State</td><td>000000000000000000000000000000000000000</td><td></td><td><u>୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶</u></td><td>200000000000000 (* (* ,</td><td>.,.(@@@@@@@@@@@@@@//@</td><td>@@,*,*%.*# ((,. (*,,</td><td>/,,*.%&/,,00000000000000000</td><td>aaaaaaaaaaaaaaaaaaaaaaaaaaa*%%%</td><td>**#%*@&@%@%</td></tr><tr><td>Processor ************************************</td><td><u>രഭരത്തെ തെ</u>ത്തെ തെ</td><td><u>ଉଦ୍ଭଭଳ୍ଲଭଳ୍ଲଭଳ୍ଲଭଳ୍ଲଭଳ୍ଲଭଳ୍ଲଭଳ୍ଲଭଳ୍ଲଭଳ୍ଲ</u>ଭୁଜୁଭୁଜୁଭୁଜୁ</td><td><u>୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦</u></td><td>200000000000000 /#(/(,</td><td>*/*@@@@@@#(@@@@#(@(#@</td><td>8@@##.%(*.*/*</td><td></td><td>aaaaaaaaaaaaaaaaaaaaa. %&#</td><td>**(,&/@@@&/</td></tr><tr><td>Presentation Presentation Presentation<</td><td><u>@@@@@@@@@@@</u></td><td></td><td></td><td>2000</td><td>0@@#@@@@@@#@</td><td></td><td>0000000000</td><td>aaaaaar</td><td>100000000000</td></tr><tr><td>Package back The package back of the package backage b</td><td>000000000000</td><td></td><td><u>ୁ</u> ବ୍ରତ୍ତ୍ରତ୍ତ୍ରତ୍ତ୍ରତ୍ତ୍ରତ୍ତ୍ରତ୍ତ୍ରତ୍ତ୍ରତ</td><td>100</td><td><u>ଜେଜଜଜଜଜଜଜ</u>ଜଜଜନ</td><td></td><td>000000000</td><td>aaaaa a</td><td>90000000000</td></tr><tr><td>Bit Bit Bit Bit Bit Bit Bit Bit Bit Bit</td><td><u> </u></td><td></td><td></td><td>20 X.*</td><td>/ (&@@@@@@@@@</td><td></td><td>000000000000000000000000000000000000000</td><td><u>@@@@@</u></td><td><u> </u></td></tr><tr><td>Particle Particle Partintee Partintee Particle Particle Particle Particle Particle Parti</td><td>0000000000</td><td>alalalalalalalalalalalalalalalalalal</td><td>୶ଡ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼</td><td></td><td>///@@@@@(((@@@at@@t@t@t@@</td><td>i Come Come Come Come Come Come Come Come</td><td>******</td><td>******</td><td>*******</td></tr><tr><td>Page depended 10/* (000 page confect on the confect on</td><td>00000000000</td><td>480000000000000000000000</td><td><u>୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦</u></td><td></td><td>#%(%(@%%@@&@&%&%@&#@@&</td><td></td><td>******</td><td></td><td>******</td></tr><tr><td>Decemponed ****(**//*****************************</td><td>ୠୠୠୠୠୠୠୠୠ</td><td><u>ନ୍ତ୍ରର୍ଭ୍ର୍ର୍ର୍ର୍୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍୍ର୍୍ର୍ର୍ର୍୍ର୍</u></td><td><u>୵ଡ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼</u></td><td>#)</td><td>/%%%/(@@@@@@@@#@&@@@%</td><td>(@@@@@(</td><td>** ,***/*/ **.*****/*/</td><td>**</td><td>*****</td></tr><tr><td>000000000000000000000000000000000000</td><td>00000000000</td><td>****(**//**********</td><td>*****</td><td>% (%</td><td>/#/(%&%%#(#((((@@@@@@</td><td>3@@@@@(</td><td>*****</td><td>** ***</td><td>****</td></tr><tr><td>000000000000000000000000000000000000</td><td>00000000000</td><td>******,/**********</td><td>****</td><td>1% (%%</td><td>*######%(#&@@@@@@@@@@@</td><td>*//</td><td>(* (,/(.* / /(/******</td><td>***/*</td><td>* **</td></tr><tr><td></td><td>ୠୠୠୠୠୠୠୠୠୠ</td><td>******** ***********</td><td>**********</td><td>(//#%#</td><td>###%#(//((@@@@@@@@@</td><td>000000</td><td>******</td><td>*****</td><td>****</td></tr><tr><td>328 3000000000000000000000000000000000000</td><td>00000000000</td><td>************</td><td>* *********</td><td>*((,(%#4</td><td><%&%##(*/(@@@@@@@@@</td><td>2000</td><td><u>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</u></td><td>200000000</td><td>P@@</td></tr><tr><td>Proceeded Proceeded Proceded Procededd Procededdd Procededddddddddddddddddddddddddddddddddd</td><td>00000000000</td><td>୵ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼</td><td>ଌ୕ୖଌଡ଼ଡ଼ଡ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ୡ</td><td>,,****,*/,</td><td><pre>/*/*##*//@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@</td><td>000000</td><td>00000000000000000000000000000000000000</td><td>୶ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼</td><td>88</td></tr><tr><td>Predeepeepeepeepeepeepeepeepeepeepeepeepee</td><td>൭൭൭൭൭൭൭൭൭൭൭൭൭</td><td><u>ୁ</u> ଅଭିତ୍ରଭିତ୍ରଭିତ୍ରଭିତ୍ରଭିତ୍ରଭିତ୍ରଭିତ୍ରଭିତ୍ର</td><td>രരത്തെയത്തെയും</td><td>, , ** , , / ((**</td><td>//*#(,(/@@@@@@@@</td><td>0.0000000000000000000000000000000000000</td><td></td><td><u>എത്തത്തത്തത്തം</u></td><td>8</td></tr><tr><td>Presence on the second on t</td><td><u>ରୁଭର୍ଭୁଭର୍ଭୁ</u>ର୍ଭ୍</td><td><u>୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦୦</u></td><td><u>ାଉ</u>ଭୁଭୁତ୍ରଭୁଭୁଭୁତ୍ର କରୁ</td><td><u> </u></td><td><u>ରଚଚଚଚଚଚଚଚଚଚଚ</u>ଚଚ</td><td>2000</td><td><u>ଉତ୍ତର୍ଭ୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର</u></td><td>000000888888</td><td></td></tr><tr><td>Predeededededededededededededededededede</td><td>0@@@@@@@@@@</td><td>ର୍ଭ୍ଭର୍ଭ୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍ର୍</td><td><u>കര്യക്തെ</u>ക്കെക്ക്ക്ക്ക്ക്ക്ക്ക്ക്ക്ക്ക്ക്ക്ക്ക്</td><td></td><td><u>କାରକାରକାରକାରକାର</u>କାର</td><td>1000000</td><td>୶୶୶୶୶୶୶୶୶୶୶୶୶୶୶</td><td></td><td></td></tr><tr><td>000000000000000000000000000000000000</td><td>൭൏൏൏൏൏൏൏</td><td><u>ରଜାଜାଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର</u> ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ୍ର ଜାନ୍ତ</td><td></td><td></td><td>രമരത്തെല്ലെക്കും</td><td>2000</td><td><u>ക്കെത്തത്തത്തത്തത്ത</u>ത്ത</td><td></td><td></td></tr><tr><td>Proceeded Procededde Procededdde Procededde Procededde Procededde Procededdedde Procededde Procededde Procededde Procededdedde Procededdde Procededdedde Procededdedde Procededddedde Procededddedde Procededddeddeddeddeddeddeddeddeddeddeddedd</td><td><u>രൂരുതത്തത്ത</u>്</td><td>୶ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲ଢ଼୲</td><td>୶ୠୠୠୠୠୠୠୠୠୠୠୠ</td><td></td><td><u>ାର(ଜ(ଜ)ର)ର(ଜ)ର(ଜ)ର(ଜ)ର(ଜ)</u></td><td>2000</td><td><u>ଜ୍ଞାନ୍ତ୍ରାର୍</u>ତ୍ତ୍ର କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ବ୍ର କ୍ରାର୍ଚ୍ଚ କ୍ରା ଭାଷା ସ୍ଥାର୍ବ କ୍ରାର୍ବ୍ଦ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ଚ୍ଚ କ୍ରାର୍ବ୍ଦ କ୍ରାର୍ବ୍ଦ କ୍ରାର୍ବ</td><td></td><td></td></tr><tr><td>000000000000000000000000000000000000</td><td>രതരത്തിന്നെ</td><td>୶୶ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼</td><td>୶ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼ଢ଼</td><td></td><td><u>പത്തില്ലെയ്തിന്നും</u> പ്രത്തിന്നും പ്രത്തിന്നും പ്രത്തിന്നും പ്രത്തിന്നും പ്രത്തിന്നും പ്രത്തിന്നും പ്രത്തിന്നും പ</td><td>2000</td><td>a@@@@@@&&&&&&</td><td>a na na za za za lin na zalini za lin linara za za za</td><td>calification of the second sec</td></tr><tr><td>0000%%&0000000000000000000000000000000</td><td><u>ବଜ୍ଜଜ୍ଜ</u>୍ଜ୍ର୍ଭ୍ର୍ର୍୍ର୍୍ର୍</td><td></td><td><u>ക്കുകള്കള്കള്കള്</u>കള്കള്</td><td><u>ଅଭୂଜାନ୍ତ୍ରରାଜନ୍ତ୍ରରାଜନ୍ତ୍ରରାଜନ୍ତ୍ର</u></td><td><u> </u></td><td>1000000</td><td>0&&&&&&&&&&&&</td><td>&@&@&@@&&&&&&&@@&@&</td><td>8888</td></tr><tr><td>.282328282828282828282828282828282828282</td><td><u>a@@%%&@@@#</u></td><td></td><td>aa*, @, @@#, @@@@</td><td>a / / # / @@@@@@@@@@@@@@@@@@</td><td>ര</td><td>0.0.0.0.0.0</td><td>888888888888888</td><td>ଌୄଢ଼ୡୠଢ଼ୡଢ଼ୡଢ଼ୡଢ଼ୡୠୡୠୡ</td><td>8.8.000</td></tr><tr><td></td><td>@@@%&#@@@@</td><td></td><td>പര്വര്വര്വര്ത്തത്തെ പ്രത്തത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ പ്രത്ത്തിന്റെ</td><td>3^{11 11 11} 11 (a)@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@</td><td>രുതതതതത്തിന</td><td>0,</td><td>8888888888888</td><td>444444444444444444444444444444444444444</td><td>88888</td></tr><tr><td></td><td>0@@@@@@@@@@</td><td>marata</td><td>000000000000000000000000000000000000000</td><td>100000000000000000000000000000000000000</td><td>000000000000000000000000000000000000000</td><td>2000</td><td>00000000000000</td><td>100000000000000000000000000000000000000</td><td>രത്തിരുത്ത</td></tr></tbody></table>					



Part I: Motivation

What data are we talking about and why is it relevant?











chairecyber-cni.orgi Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)



Two Use Cases



Self-Driving Cars Industry 4.0













Tesla Autopilot 2.0 (Camera View) - Level 5 Autonomy. Full Self-Driving Hardware Daniel

Published on 19 Nov 2016

https://www.youtube.com/watch?v=V4PDTD2VHSU Tesia Autopilot 2.0 (Camera View) - Level 5 Autonomy. Full Self-Driving Hardware

1111

LEFT REARWARD VEHICLE CAMERA

33

Armit

MEDIUM RANGE VEHICLE CAMERA

RIGHT REARWARD VEHICLE CAMERA

ROAD LIGHTS

OBJECTS

ROAD SIGNS



Waymo 360° Experience: A Fully Self-Driving Journey Waymo Published on 28 Feb 2018 https://www.youtube.com/watch?v=B8R148hFxPw





Eye tired Wawn eat cigar

s building an all-seeing surveillance stat Washington Post Published on 7 Jan 2018 https://www.youtube.com/watch?v=uReVvICTrCM









Data Processing Pipeline

Prevent Security-by-Design

Detect Anomaly Detection

Mitigate Self-Defend Security Incidents Self-Recover from Security Incid

data on my side data with somebody else



11

No mass-surveillance



Security

Local Processing in the car



Data Sharing

Benefit from collaboration



Versatility

Remote Processing in the cloud









Lots of research challenges: Trust





https://youtu.be/k5eL_al_m7Q





















Synthesis of Distributed Observations

Data Sharing / Synergies e.g. remote maintenance

Microservice

Inter-Node Comm. Interface

Industry 4.0 Site

Service Runtime Environment

Distribut



Management Se etwork natio



16

No unnecessary exposure



Security

Local Processing in the factory



Data Sharing

Benefit from collaboration



Versatility

Remote Processing in the cloud









When **Data** is the new **Oil**, Security is the Blowout Preventer

We **need data sharing**. But it has to be **secure** = responsible, transparent, secured,



Marc-Oliver Pahl, IMT Atlantique Rennes

Chair holder Chaire Cyber CNI

Co-Directeur Equipe IRIS / UMR LAB-Sticc Digital Teaching Coordinator German-French Academy for the Industry of the Future Leader of the Smart Space Orchestration Team at TUM Vice President German Chapter of the ACM









Annossys SI BNP PARIBAS SCEDE NOKIA Bell Labs

Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)



Part II: Security in the Wild Terminology, goals chairecyber-cni.org/











Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)





Pahl | Al4Industry Security Keynote

CHAIRE CYBERCNI Sécurité des infrastructures critiques



Purdue Enterprise Reference Model (PERA) [1]

1990 Williams; NOW **ISA-99** (ISA / IEC 62443)



Pahl | Al4Industry Security Keynote



21

Originally: ICS vs IIoT

- IoT = Things connected to the Internet
- ICS = Explicitly NOT connected to the Internet





Why do we need Security?

- safety
- health
- welfare
- financial losses (production stop)
- lawsuit (non-compliance)
- environmental impact (oil spill)
- security (access control)

Pahl | Al4Industry Security Keynote

. . .



Fundamental Problem

- Disconnected legacy systems get connected to the Internet
- Large attack potential
 - remote
 - script kids
 - hackers
 - stuxnet even over air gap

Pahl | Al4Industry Security Keynote CYBERCN



A. Stuxnet

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.



2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilitiessoftware weaknesses that haven't been identified by security experts.



In the beginning, Stuxnet spies on the

uses the information it has gathered to

take control of the centrifuges, making

them spin themselves to failure.

operations of the targeted system. Then it

5. control





Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.



Pahl | Al4Industry Security Keynote



3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



6. deceive and destroy

When?

- By whom?
- Where?
- Target?
- How?
 - What vulnerabilities are exploited?
 - How is the attack flow?
- Success rate?







B. Flame





Pahl | Al4Industry Security Keynote

• When?

- By whom?
- Where?
- Target?
- How?
 - What vulnerabilities are exploited?
 - How is the attack flow?
- Success rate?





HAVEX Infection Chain



These malicious software are downloaded by target companies, giving attackers access to their networks.



hosted in these websites.



vendor sites.

C. Havex



- When?
- By whom?
- Where?
- Target?
- How?
 - What vulnerabilities are exploited?
 - How is the attack flow?
- Success rate?



27

D. BlackEnergy





Pahl | Al4Industry Security Keynote

- When?
- By whom?
- Where?
- Target?
- How?
 - What vulnerabilities are exploited?
 - How is the attack flow?
- Success rate?



28

Skills for ICS Cybersecurity?

- Requires Multidisciplinary understanding
 - Cybersecurity: networking stack / OS stack
 - Functionality of ICS
 - Physics / Engineering requirements of industrial processes





What are **advantages** and disadvantages of having (networked) PLCs?

- Good
 - Software can easily be exchanged adapted
 - Mass production as "general purpose" -> cheaper
 - Flexible (can be adapted)





What are advantages and **disadvantages** of having (networked) PLCs?

- Bad
 - Software can easily be exchanged adapted (= modified by attack)
 - All software problems such as dead locks, overflows, timing issues, ...
 - Much bigger attack surface
 - The weakest part in the chain defines the security level
 - Older devices were not designed with properties that spread from IT networks such as high traffic and fail or reset then
 - Human-factor: Knowledge in IT and OT rare -> common security standards are not taken into account

Pahl | Al4Industry Security Keynote



31

Goal for ICS security

- ensure the safe and reliable operation of the physical process [1]
 - Catastrophic safety failures
 - Environmental release of hazardous materials
 - Loss of production
 - Product recall
 - Regulatory fines
 - Sustained production inefficiency
 - Loss of public confidence"

Pahl | Al4Industry Security Keynote

CYBERCN



ICS Security Standards

- ISA-84
- IEC 61508
- ISA-95
- ISA-99 (ISA-62443 / IEC 62443)
- NERC CIP
- 6 CFR 27
- Homeland Security's Chemical Facility Anti-Terrorism Statutes (CFATS)

Pahl | Al4Industry Security Keynote CYBERCNI

. . .

 \bullet



A. Worcester air traffic communications

Worcester air traffic communications In March 1997, a teenager in Worcester, Massachusetts, disabled part of the public switched telephone network using a dial-up modem connected to the system. This knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activated runway lights were shut down, as well as a printer that controllers used to monitor flight progress. The attack also knocked out phone service to 600 homes and businesses in the nearby town of Rutland. (http://www.cnn.com/TECH/computing/9803/18/ juvenile.hacker/index.html)



- When?
- Who?
- What attacked?
- How?
- Impact







B. Maroochy Shire sewage spill

Maroochy Shire sewage spill In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a two-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks. (http://csrc.nist.gov/groups/ SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf and http://www.theregister.co.uk/2001/10/31/ hacker_jailed_for_revenge_sewage/)

- When?
- Who?
- What attacked?
- How?
- Impact



ed?



C. Davis-Besse Nuclear plant

Davis-Besse In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked. (http:// www.securityfocus.com/news/6767)

- When?
- Who?
- What attacked?
- How?
- Impact







Some Literature to continue...

- Weapon. Crown Publishing Group, USA.
- Alex Gibney, Zero Days (2016) movie: https://youtu.be/2qaxJs8wYVw
- Exposed: Industrial Control Systems".
- cyber-kill-chain-36297

• Kim Zetter. 2014. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital

• [1] Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt. "Hacking

• [2] Keith Stouffer (NIST), Suzanne Lightman (NIST), Victoria Pillitteri (NIST), Marshall Abrams (MITRE), Adam Hahn (WSU), "SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security," Mai 2015, NIST, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

• [3] Michael J. Assante and Robert M. Lee, "The Industrial Control System Cyber Kill Chain," October 2015, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-



37

Security Mechanisms and Risks



from: Jelena Misic and Vojislav B. Misic, "Wireless personal area networks : ² Pahl Ald Interformance, interconnections and security with IEEE 802.15.4," 2007



 \triangleleft \triangleleft 2 \triangleleft \bigcirc

Sinkhole (DoS) Blackhole

attacks

Grayhole (DoS)

Selective forwarding

Wormhole

Sybil

Collision

Battery exhaustion

Unfairness

Sleep Deprivation

Jamming (DoS)

Node tampering

38

Part III: Where to use AI? Examples where AI can help











chairecyber-cni.orgi Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)





Prevent Security-by-Design



T7: Autoencoder Integrity Authentication

T4: Non-Cooperative Game Possibility for defense

T3: CVE -> Graph NLP Semantic Processing

> **T5: SDN Security** Self-Security Policy-based Security

A















Going to the full stack



People **Interface Devices**

Orchestration Workflows, etc.

Context Manage

Bidirectional Adaptation

Heterogeneous **Smart Devices**

Physical World



Sensor

Service

Actuator



People **Interface Devices**

Orchestration Workflows, etc.

Context Managem

Bidirectional Adaptation

Heterogeneous **Smart Devices**

Physical World





I. Prevent Identities, Secure Metadata, Access Control













chairecyber-cni.orgi Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)







Distributed Smart Space Orchestration System







People **Interface Devices**

Orchestration Workflows, etc.

Context Managem

Bidirectional Adaptation

Heterogeneous **Smart Devices**

Physical World

Service



II. Detect & Mitigate -> Prevent in the Future Machine-Learning-based Modeling and Sandboxing using Anomaly Detection









chairecyber-cni.orgi Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)

Annossys S BNP PARIBAS SCEDE NOKIA Bell Labs















Management $(\cap$ etwork Internatio





- Passive traffic monitoring
- Behavior modeling using Machine **Prevent**

Security-by-Design

Detect Anomaly Detection

Mitigate Self-Defend Security Incidents Self-Recover from Security Incide



ML-Based Clustering of Periodicities



Pahl | Al4Industry Security Keynote





People **Interface Devices**

Orchestration Workflows, etc.

Context Manage

Bidirectional Adaptation

Heterogeneous **Smart Devices**

Physical World

UI Service Service

notify subscribe set get

Gateway

Sensor

Actuator



III. Protect SW & HW **Anomaly Detection and Sandboxing, Watermarking**













chairecyber-cni.orgi Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)

















Management $(\cap$ etwork Internatio



People **Interface Devices**

Orchestration Workflows, etc.

Context Manage

Bidirectional Adaptation

Heterogeneous **Smart Devices**

Physical World



How China is building an all-seeing surveillance state Washington Post Published on 7 Jan 2018 https://www.youtube.com/watch?v=uReVvICTrCM

88

SUV

- -

- aretia

- 區机結车





"We knew the world would not be the same. A few people laughed, a few people cried. Most people were silent. I remembered the line from the Hindu scripture, the Bhagavad-Gita; Vishnu is trying to persuade the Prince that he should do his duty, and to impress him, takes on his multi-armed form and says, 'Now I am become Death, the destroyer of worlds.' I suppose we all thought that, one way or another."

- J. Robert Oppenheimer (Researcher/ Head Manhatten Project)







CHAIR OF YBERCN **Critical National Infrastructures**

OA

You are always welcome to contact us



3rd Summer School Future-IoT: IoT meets Security Oct 5-9, 2020, Strasbourg -> school.future-iot.org

neymoles and challenges

ron our industry partners!





IMT Adantique Bretagne-Pays de la Loire cole Mines-Télécom

rom our industry partnersi

82

E

newnoles and challenges

SPACE

Technical University of Munich



CARN Télécom & Société numérique lelecom & societe numerique

Université anco-allemande lochschule

elm.leblanc



Apply now! school.future-iot.org



Cybersecurity of Critical Infrastructures



Some Methods MACHINE and **Block**chain

Prevent Security-by-Design







Pahl | Al4Industry Securit, Keync AIRBUS



LEARNING Digital**Twin**





Mitigate

Self-Defend Security Incidents Self-Recover from Security Incidents

> Chaire Cyber CNI 5 industrial partners 8+ associated researchers 12 PhD students (2020/5)

CHAIRE

CYBER CNI

urité des infrastructures critiques

EST. 2016

