



Network Security in the Age of Cyberwarfare

Robert Barton, P. Eng
Distinguished Systems Engineer, Cisco
February 8, 2019



Hackers can Freeze You True or False?




Hackers can Freeze You True

Security

Finns chilling as DDoS knocks out building control system

Hint: next time, buy a firewall *before* you're attacked

By Richard Chirgwin 9 Nov 2016 at 03:30

17  SHARE ▼



Residents in two apartment buildings in the Finnish town of Lappeenranta had a chill-out lasting more than a week after a DDoS attack battered unprotected building management systems.



https://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/

Your Car Can be Hacked and Remotely-Controlled (while you're driving it) True or False?



Your Car Can be Hacked and Remotely-Controlled (while you're driving it)

True



<https://www.kaspersky.com/blog/remote-car-hack/9395/>

Your Pacemaker Can Be Hacked and Could Kill You True or False?



Your Pacemaker Can Be Hacked and Could Kill You True



A screenshot of the U.S. Food & Drug Administration (FDA) website. The page is titled 'Medical Devices' and features a sub-section for 'Safety Communications'. The main headline reads: 'Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication'. Below the headline are social media sharing options for Facebook, Twitter, LinkedIn, Pinterest, Email, and Print. The 'Date Issued' is listed as January 9, 2017. The breadcrumb trail at the top of the content area reads: Home > Medical Devices > Medical Device Safety > Safety Communications. The left sidebar contains a 'Safety Communications' menu with links for '2018 Safety Communications' and '2017 Safety Communications'. The top navigation bar includes links for Home, Food, Drugs, Medical Devices, Radiation-Emitting Products, Vaccines, Blood & Biologics, Animal & Veterinary, Cosmetics, and Tobacco Products. The search bar at the top right contains the text 'Search FDA' and a magnifying glass icon. The top of the page features the U.S. Department of Health and Human Services logo and the text 'U.S. FOOD & DRUG ADMINISTRATION'. There are also links for 'A to Z Index', 'Follow FDA', and 'En Español'.

<https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm>

The Age of Cyber Warfare has Arrived

Increasing Industrial Threats



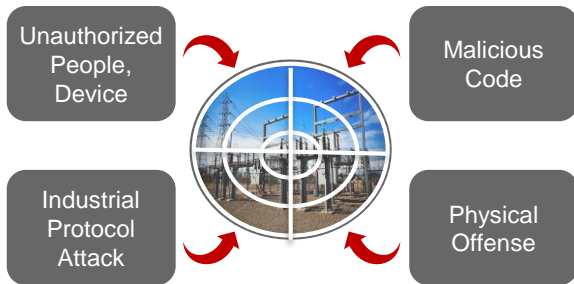
German Steel Mill
Cyber attack (2014)



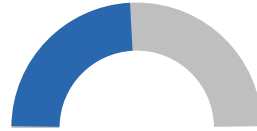
Cyber attack on Saudi
Aramco (2012)



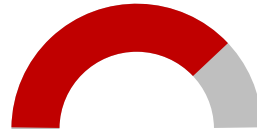
151 Cyber Incidents led to
power outage or disruptions
in 2014 US*



Customer Having Gaps



49% of BDM site security is among
top application challenges*



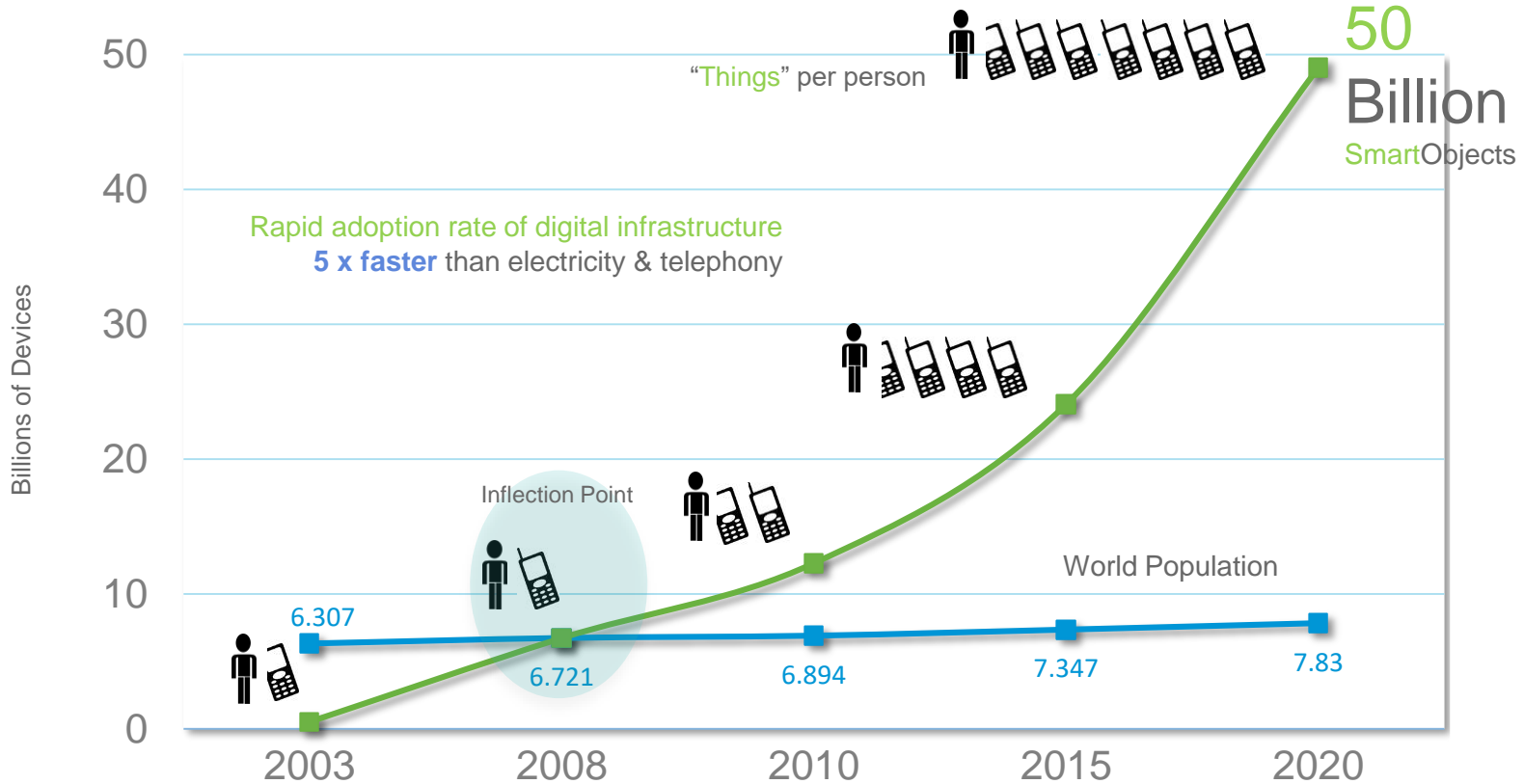
78% of IT security staff lack
visibility & management to secure
IoT devices*

Compliance Mandating



- Cyber and Physical Security
- Mandate for NA Power Utilities BES
- Referred by global Utilities, also other verticals

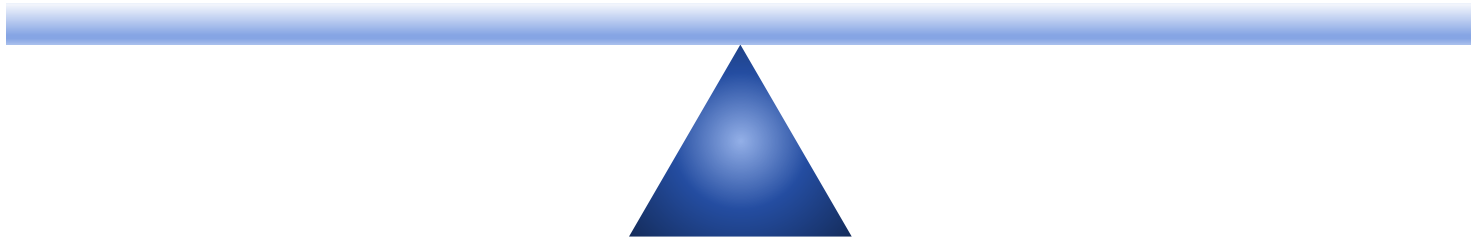
The Increase of Connected Things



Striking a Balance

Usability /
Connectivity

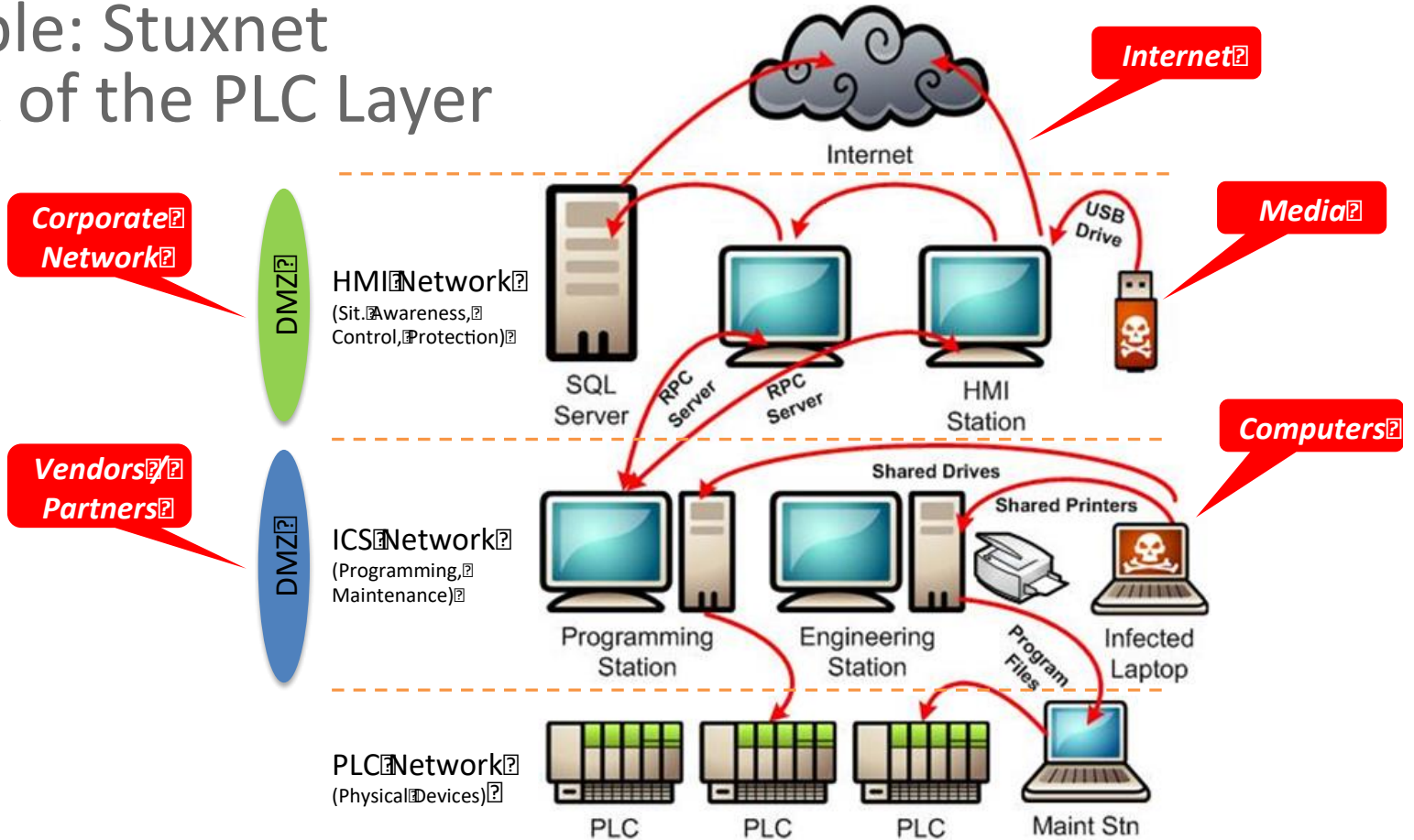
Security



Weak and Old Protocols: Supervisory Control and Acquisition of Data (SCADA)

- SCADA was created in the 1960s
- Initially designed to carry data over serial
- Commonly found in industrial settings
- Client / Server architecture
- Evolved over the years to adapt to IP transport
- Security was not part of the original design, and SCADA has changed very, very little!

Example: Stuxnet Attack of the PLC Layer



What was so special about Stuxnet?



The first rootkit targeting ICS



Exploited four zero-day vulnerabilities in the dropper



Compromised two digital certificates



Ability to inject code into PLC

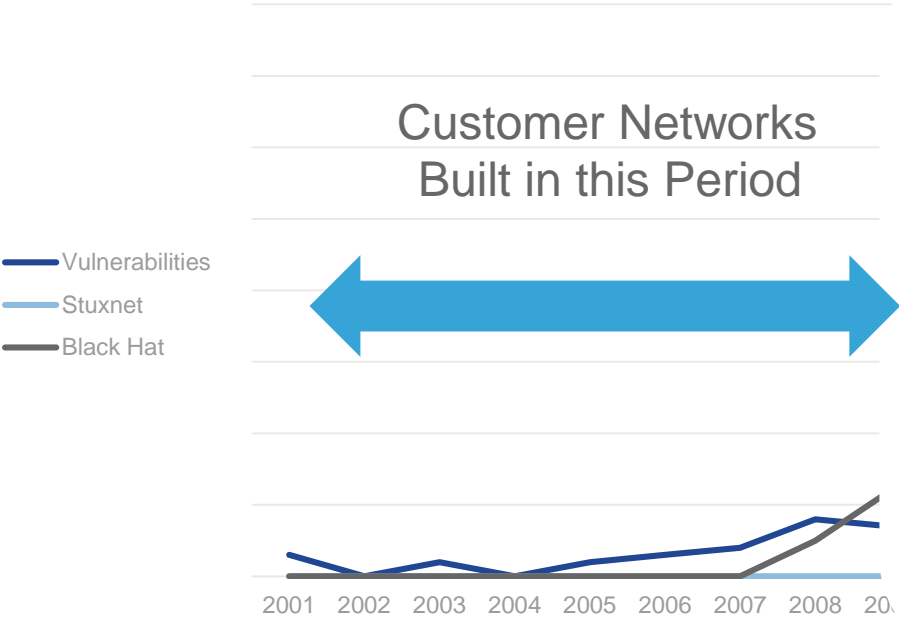


Hide from control system operators



Remotely controlled by CC or act autonomously

Why Security Must Change



The Impact of Stuxnet

Destroyed Uranium centrifuges



Ruptured oil pipeline



Manipulated steel mill equipment



Impact of cost can be millions of dollars

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

Case Study: Ukraine Substation Industrial **Attack**

- 3 Ukrainian power distribution companies
- 30 sub-stations disconnected
- 225K customers lost power for hours
- Attackers remotely controlled SCADA DMS



Ukraine Grid Attack – Chronology of Events

Spear phishing to gain business network access



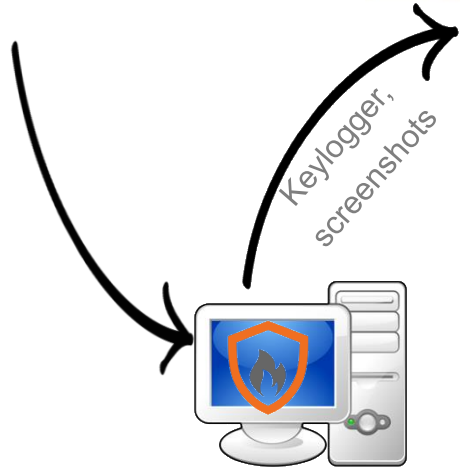
Theft of Credentials



Remote operation of ICS Systems



KillDisk to erase MBR and delete targeted logs



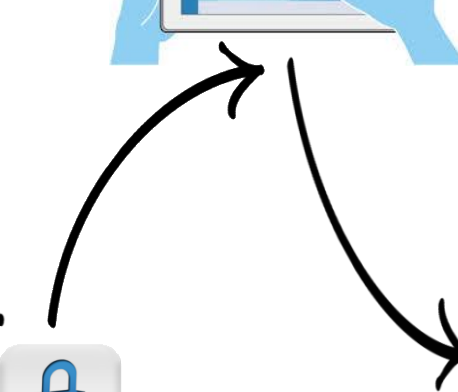
Keylogger, screenshots



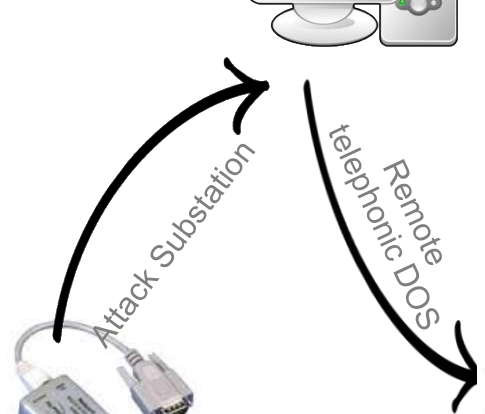
BlackEnergy 3 malware installed



Use of VPNs to access ICS network



S2E devices compromised at firmware level



Attack Substation

telephonic DOS



Power Outage

Ukraine Grid Attack – Kill Chain

Spear phishing to gain business network access



Theft of Credentials



Remote operation of ICS Systems



KillDisk to erase MBR and delete targeted logs



Attack on IT Domain

Attack on OT Domain



BlackEnergy 3 malware installed



Use of VPNs to access ICS network



S2E devices compromised at firmware level



Power Outage

Recognize This?



Ooops, your files have been encrypted! English



What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **Send \$300 worth of bitcoin to this address:**
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants



Laurence Frost and Naomi Tajitsu, Reuters

May. 15, 2017, 1:25 PM 🔥 2,528



FACEBOOK



LINKEDIN



TWITTER



EMAIL



COPY LINK

Renault-Nissan said on Monday that output had returned to normal at nearly all its plants, after a global cyber attack caused widespread disruption including stoppages at several of the auto alliance's sites.



ATTEND

TRAININGS

BRIEFINGS

ARSENAL

FEATURES

SCHEDULE

BUSINESS HALL

SPONSORS

PROPOSALS

▶ BACK

ON THIS PAGE

PRICING

OVERVIEW

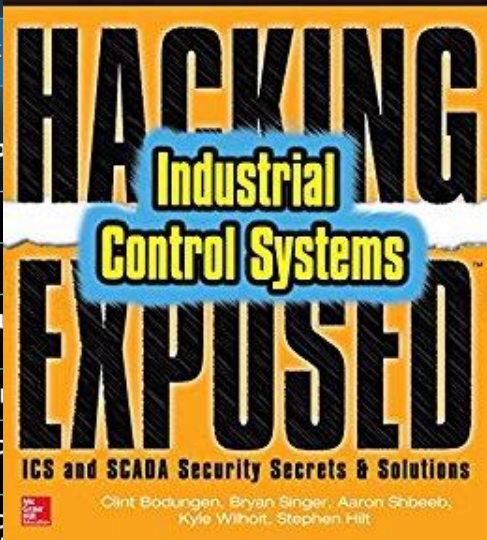
WHO SHOULD
TAKE THIS COURSE

STUDENT REQUIREMENTS

WHAT STUDENTS
WILL BRING

WHAT STUDENTS
WILL BE PROVIDED WITH

TRAINERS



REGULAR

\$5,100

ENDS JULY 13 2359 PT

HACKING SCADA/
INDUSTRIAL CONTROL
SYSTEMS

Christopher Atkins

This is not your traditional SCADA/ICS/IIoT security course! How many courses send you home with a \$500 kit including your own PLC and a set of hardware/RF hacking tools?!? This course teaches hands-on penetration testing techniques used to test individual components of a control system, including embedded electronic field devices, network protocols, RF communications, Human Machine Interfaces (HMIs), and various forms of master servers and their ICS applications. Skills you will learn in this course will apply directly to systems such as the Smart Grid, PLCs, RTUs, smart meters, building management, manufacturing, Home Area Networks (HAN), smart appliances, SCADA, substation automation, synchrophasors, and even IIoT. This course is structured around the formal penetration

The background features a dark blue gradient with intricate, wavy patterns of lighter blue and yellow lines that create a sense of depth and movement, resembling a stylized wing or a complex data visualization.

The Encrypted Traffic Problem

The

KuvatON.com



Network Threats are Evolving to Leverage Encryption

In the past 12 months:

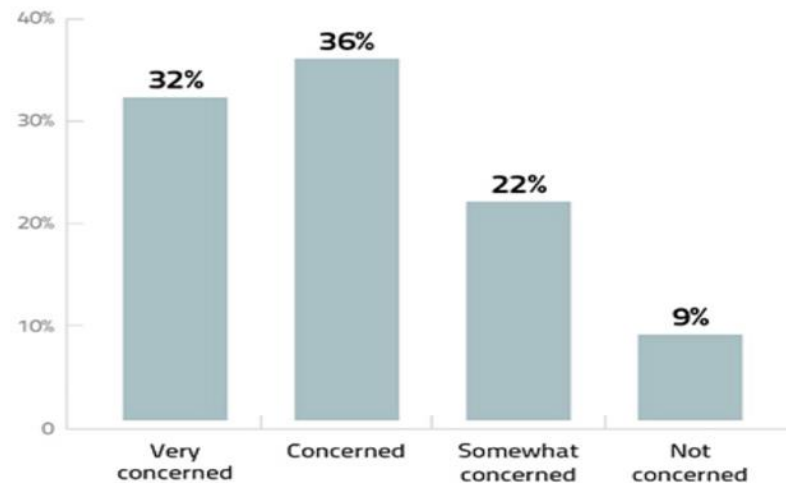
80%
have been victims
of cyberattacks or
malicious insiders

41%
of these attacks used
encryption to evade
detection

SOURCE: "HIDDEN
THREATS IN ENCRYPTED
TRAFFIC," PONSOM
INSTITUTE, AUGUST 2016,
BASED OFF RESPONSES
FROM 1,023 IT AND IT
SECURITY PROFESSION-
ALS IN NORTH AMERICA,
EMEA; ARTWORK:
YAPANDA/ISTOCK



How concerned are you that encrypted communications
leave your network vulnerable to hidden threats?



Encrypted Traffic Analytics

Overview

Malware Detection and Visibility without Decryption



Malware in Encrypted Traffic

Is the payload within the TLS session malicious?

- End to end confidentiality
- Channel integrity during inspection
- Adapts with encryption standards



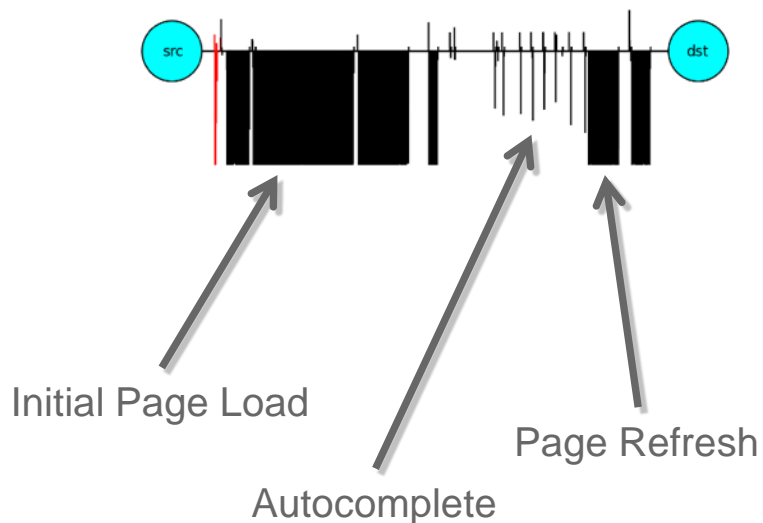
Cryptographic Compliance

How much of my digital business uses strong encryption?

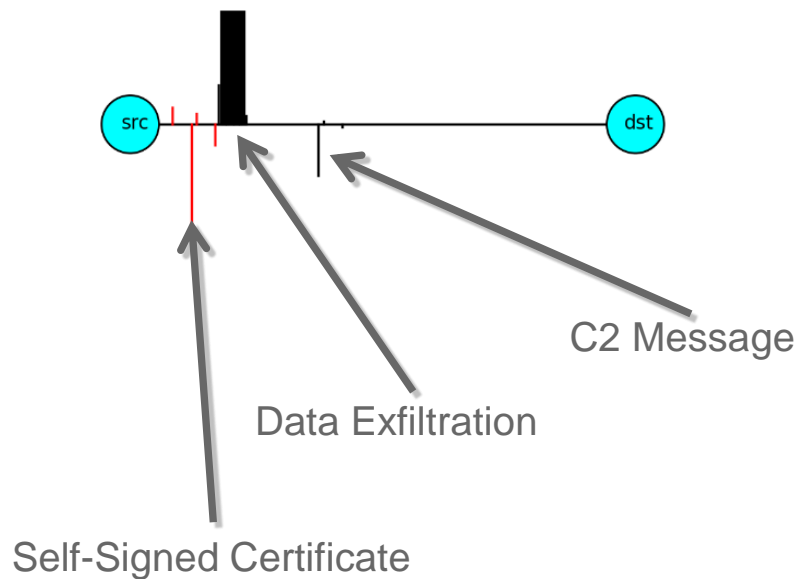
- Audit for TLS policy violations
- Passive detection of Ciphersuite vulnerabilities

Detecting Malware by Behavioral Analytics (ML/AI)

Google Search



Bestafera



In Summary

- The world has become hyper-converged and the attack surface is massive
- Left unprotected, industrial systems are the most vulnerable
- Attackers are using Ransomware style attacks at an alarming rate
- The move to encrypted traffic is ushering in a new era of AI-based network security

Thank you.

