

ICS Vendors Still Epic Fail

Jonathan Pollet
Red Tiger Security

ISF Summer Meeting – July 4, 2019

Jonathan Pollet – CISSP, PCIP, CAP

- 23 Years of Electrical Engineering, SCADA, Industrial Controls, and IT Experience
  - PLC Programming and SCADA System Design and Commissioning
  - Wireless RF and Telecommunications Design and Startup
  - Front-end Web Development for SCADA data
  - Backend Database design for SCADA data
  - Acting CIO for Major Oil Company for 2 years – Enterprise IT Management
- Last 18 Years Focused on SCADA and IT Security
  - Published White Papers on SCADA Security early in 2001
  - Focused research and standards development for SCADA Security since 2002
  - Conducted over 250 security assessments on Critical Infrastructure systems
  - Conducted over 150 International conferences and workshops on CIP
  - Developed safe security assessment methodology for live SCADA Systems
  - Co-developed the SCADA Security Advanced 5-day training course
  - Trained over 2500 Professionals Globally
  - Featured presenter on Fox News Live, CNBC, Vanity Fair, Popular Mechanics, CIO Magazine, and several security publications

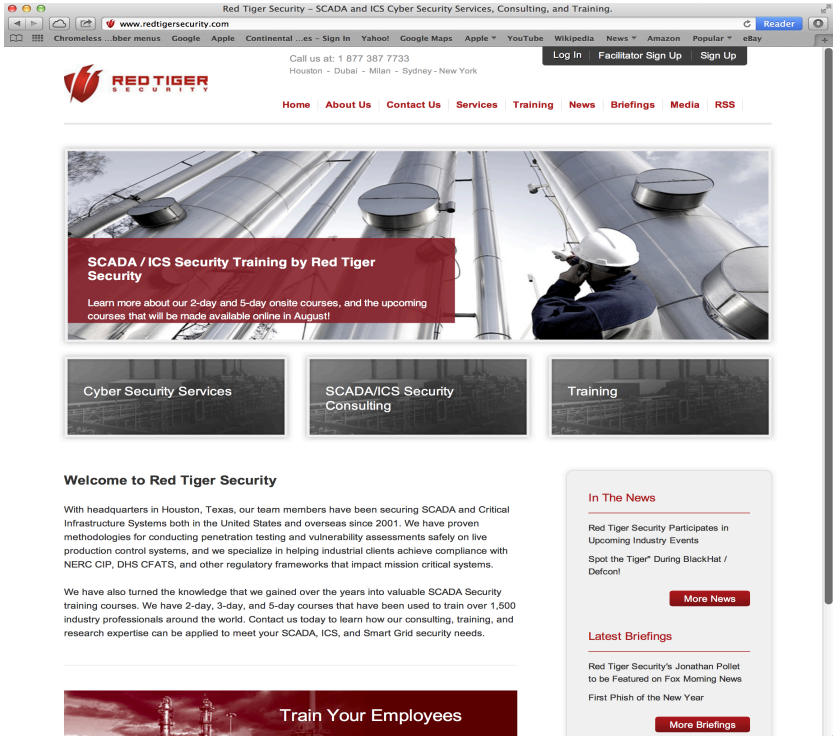
© Copyright Red Tiger Security – Do not print or distribute without consent.

Red Tiger Security

- **Consulting**
  - Penetration Testing
  - Cyber Vulnerability Assessments
  - Network Architecture Analysis / Design
  - Compliance / Security Controls Consulting
  - Cyber Security Advisory Services and Strategic Consulting
  - Development of ISA/SCADA Test Beds (US National Test Bed, Malaysia, Qatar, University of Tulsa, University of Houston, and several private industry clients)

- **Training**
  - 5-Day Advanced Security Course for Critical Infrastructures
  - 2-Day SCADA Security Course (BlackHat)

- **Research**
  - Applicability and Usability of Cyber Security Solutions for SCADA / ICS
  - Product Evaluations
  - Various DHS Research Initiatives for ICS
  - Standards Development (NERC CIP, NIST CSF, NESA (UAE), Oman Critical Infrastructure Standard, ISA99/IEC62443)



© Copyright Red Tiger Security – Do not print or distribute without consent.

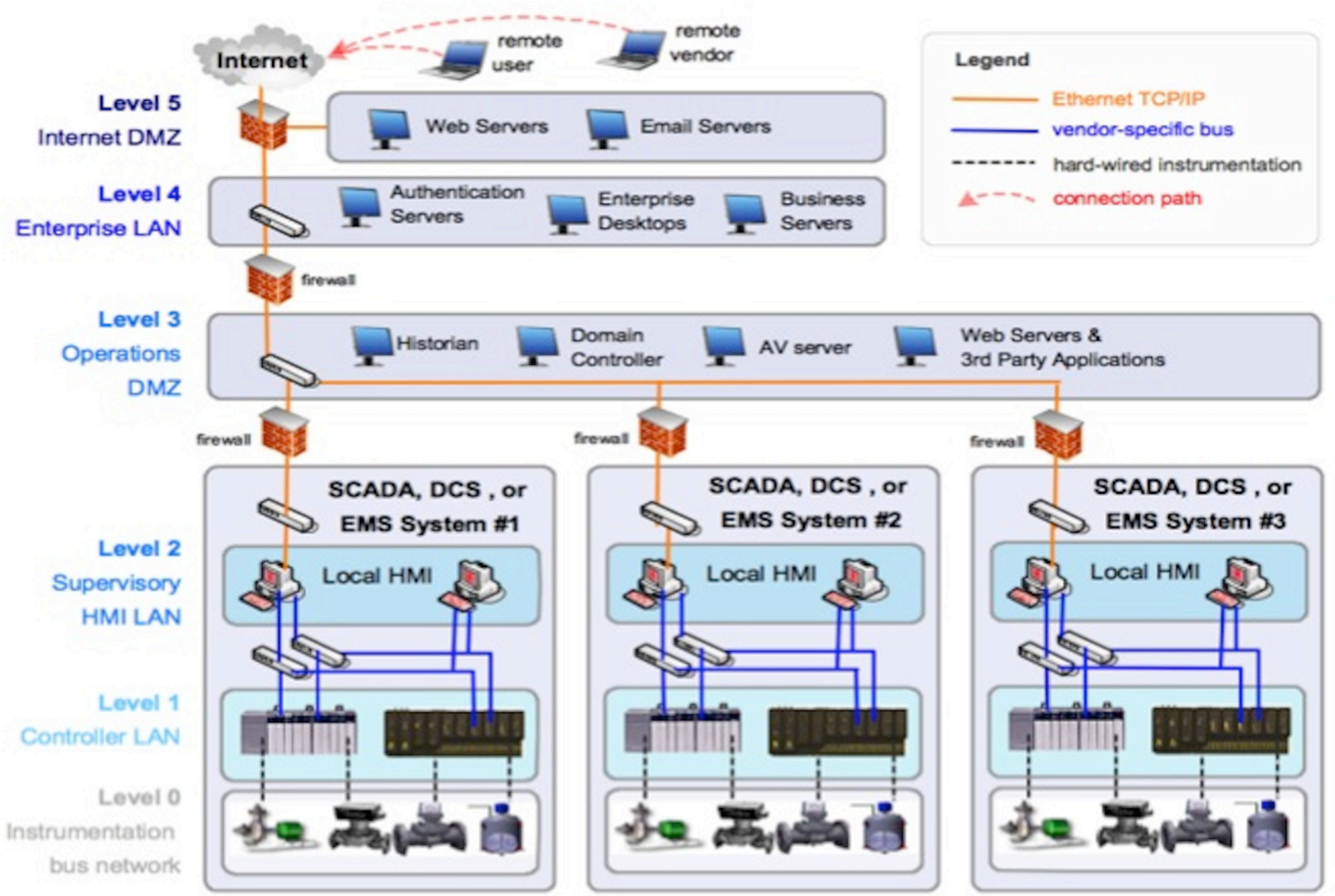
Outline

- Quick recap of missing security features in ICS embedded devices
- ICS embedded devices compared to IT network devices
- IT Printers Compared to IT Computers and Network Devices
- Hacking examples leveraging network-connected printers
- Security Strategy HP Developed to make printers an "**Equal Secure Citizen** on the network with PCs and Servers"
- Parallel lessons that can be applied to ICS embedded devices

Quick Disclaimer: the comments during my presentation are my own and does not represent any formal claims or comments from HP

© Copyright Red Tiger Security – Do not print or distribute without consent.

Where ICS Embedded Devices "Should" live in the Network



© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Controls Missing in ICS Embedded Devices

1. Lack of Authentication (anyone can connect to ICS embedded devices from anywhere and anytime)
   - View, modify, or **delete internal memory registers**
   - View, modify, or **delete internal ladder logic** or logic routines
2. Lack of Encryption (almost all embedded device protocols are clear text which means…)
   - Communications with ICS embedded devices can be **viewed, intercepted, injected, manipulated, or diverted** by anyone on the same network segment or by a malicious injected bit stream that can be routed into the network remotely

© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Controls Missing in ICS Embedded Devices

3. Monitoring Capabilities are Weak (if offered by the vendor)

- Most embedded ICS devices do not offer SNMP, and if they do, it is a vulnerable version 1 or 2 version of SNMP.
- The few SNMP MIB traps offered are not security related
- **No current elegant way to monitor the health, performance, and security of ICS embedded devices** from a centralized solution that can also monitor the same parameters from the network and host devices.

© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Controls Missing in ICS Embedded Devices

4. Lack of Forensic Capabilities
   - Security events are not logged to a common industry standard format like syslog
   - Any forensically interesting data, **if made available by the vendor, are often stored in obscure memory locations** (like 600XXX registers in Modicon)

5. No Ability to Customize Available Services (Disable Internal Web Server, TELNET, or FTP service)
   - Almost all ICS Embedded devices come standard with an internal web service running on the device. Many also contain highly vulnerable services like TELNET and FTP, and **these services can not be turned off**. These are often not required for the functioning of the device.

© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Controls Missing in ICS Embedded Devices

6. Memory Protection and Code Whitelisting

- All of the ICS embedded devices that we tested do not currently have a method to protect access to its internal data memory registers**. Some may provide a password to protect changing the logic, but the data can still be overwritten.** What happened to the hard “keys” that were required to change the logic? Or to change the processor from RUN to PROGRAM?

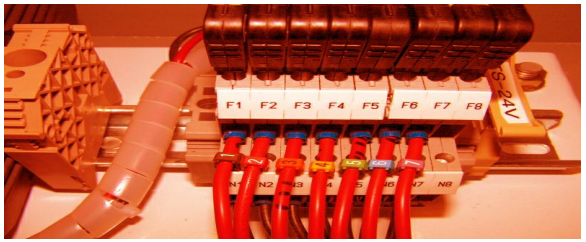
7.Elegant Asset Inventory and Rouge Device Detection

- Most PLC / ICS embedded devices do not offer an elegant way to manage all embedded devices on the network, detect new devices placed on the network, and enable common security policy deployment to them.

© Copyright Red Tiger Security – Do not print or distribute without consent.

We can learn from the standardization that has already happened on the IT side





- IT Devices today already support:
  1. Authentication (yes)
  2. Encryption (yes)
  3. Device Monitoring (SNMP3)
  4. Service Enable/Disable (yes)
  5. Forensics (yes)
  6. Code locking (with enable password)
  7. Asset Management / Rouge Device Detection (yes)

- ICS devices support?
  1. Authentication (not really)
  2. Encryption (no)
  3. Device Monitoring (maybe SNMP1 or 2)
  4. Service Enable/Disable (no)
  5. Forensics (no)
  6. Code locking (not really)
  7. Asset Management / Rouge Device Detection (vendor dependent)

© Copyright Red Tiger Security – Do not print or distribute without consent.

One large IT Vendor (HP) recognized this gap with their own embedded devices





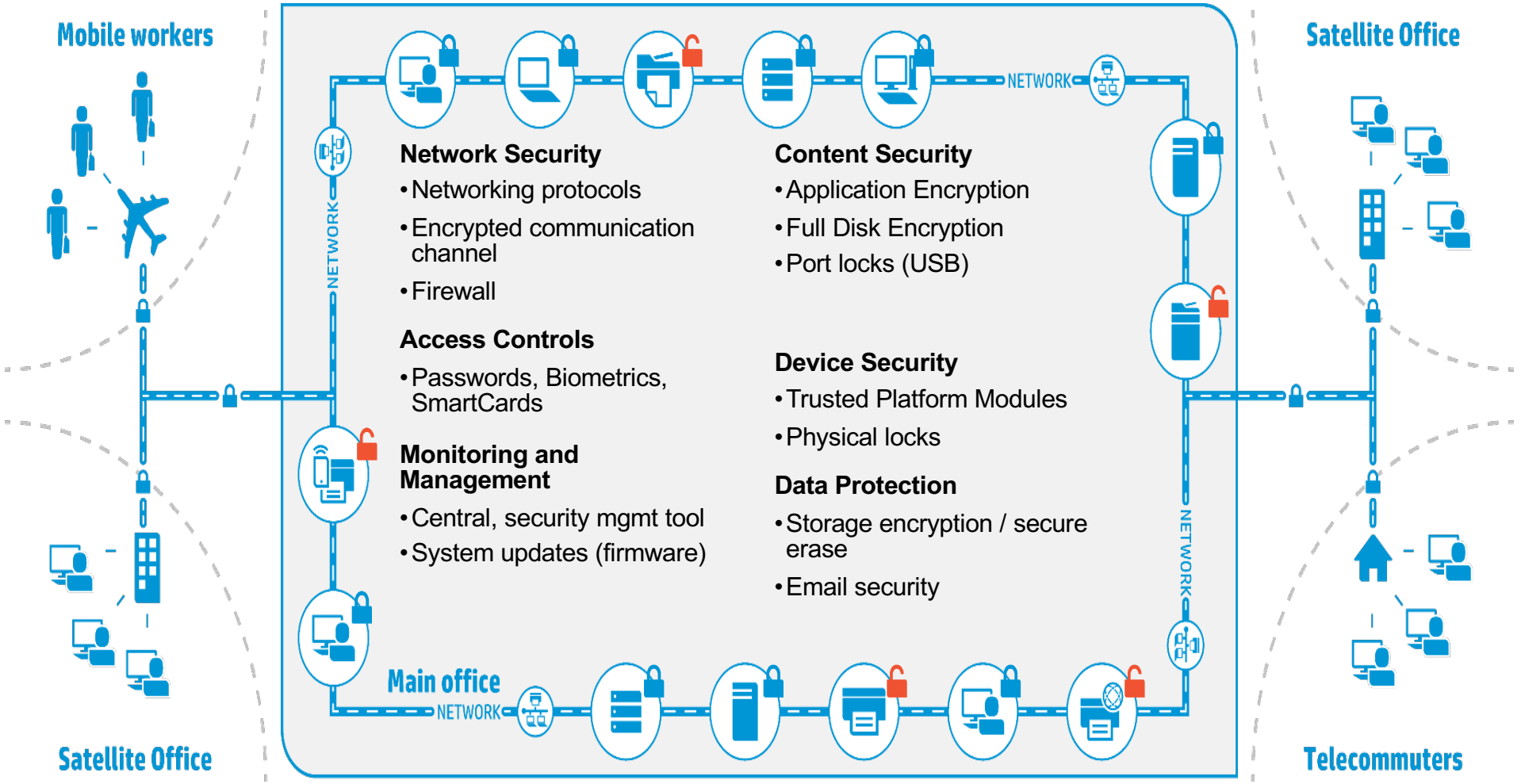
- IT Devices today already support:
  1. Authentication (yes)
  2. Encryption (yes)
  3. Device Monitoring (SNMP3)
  4. Service Enable/Disable (yes)
  5. Forensics (yes)
  6. Code locking (with enable password)
  7. Asset Management / Rouge Device Detection (yes)

- Before 2014, Printers support?
  1. Authentication (not really)
  2. Encryption (no)
  3. Device Monitoring (maybe SNMP1 or 2)
  4. Service Enable/Disable (no)
  5. Forensics (limited)
  6. Code locking (not really)
  7. Asset Management / Rouge Device Detection (limited)

© Copyright Red Tiger Security – Do not print or distribute without consent.

All Network-connected devices should be equal **Secure Citizens** on the network

Network-connected printers represented a gap when compared to PCs.



© Copyright Red Tiger Security – Do not print or distribute without consent.

HP Recognized Security Gaps in Typical Network Printers

Network Security

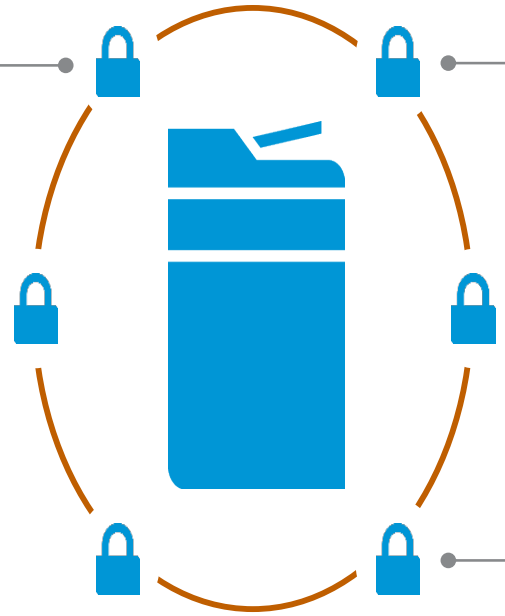
- No Security in communications to/from the device
- No Device-level Firewall
- No Certificates

Data Protection

- Print queue data storage in the clear
- Scanned data capture in the clear
- No Content Monitoring & Management

Monitoring and Management

- Limited fleet asset inventory capabilities
- Non-standard logging of events
- Firmware updates manual process
- Devices could be added to the network and not be detected
- Device monitoring very limited



Content Security

- Documents left in the tray for anyone to access

Access Controls

- Directory systems such as LDAP and AD not fully supported
- Printers are islands of devices that accept print jobs from any IP address

Device Security

- USB and network ports default to open to any connection

© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Incidents Involving Printers

- Insider trading based on info printed by someone else
  - Employee of an investment branch in large New York bank, read what his colleagues were printing on a shared printer by his desk.
  - The printouts contained data about upcoming mergers and investment decisions.
  - The employee used the information for his own trading without ever removing the print jobs from the actual printer & made around $7M.
  - The bank was fined for insider trading & the employee was sent to prison for several years.

© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Incidents Involving Printers

- Spoof Source Email
  - In 2002, at a large IT company, a disgruntled employee used an MFP (Multi-Purpose Printer) for a Scan-To-Email job to several recipients of the press. As the sender, he entered the email address of the CEO. The document contained some embarrassing text that was received as an official press note from the CEO of that company.
- MFP hard drive used as mp3 file server
  - At a university in the UK, students were using the on-campus MFP hard disks as mp3 file servers.
  - How this can be done: Using Hijetter
- Using Network Connection to Sniff Traffic
  - During a troubleshooting phone call with the printer vendor, an employee discovered a network hub and notebook was installed in the cupboard next to a printer. It was running a sniffing program and was logging all print jobs and network traffic.

© Copyright Red Tiger Security – Do not print or distribute without consent.

Printer Connection Used to Access ICS Network Segments

Internal Penetration Testing Exercise

- Printers are often installed with access to multiple network subnets so multiple departments can utilize the printer
- Printers are also excellent places for planting WiFi devices for remote access, or sniffing traffic for collecting and cracking passwords



© Copyright Red Tiger Security – Do not print or distribute without consent.

Security Incidents Involving Printers

- Corporate IT Printer Used to Access Secured VLANs
  - A network-connected MFP was left installed with default settings, which allowed an attacker to copy and execute a rootkit on the hard drive in the printer. The printer was setup with ACLs to be an active device on all of the VLANs on the corporate IT network. The rootkit allowed the attacker to enumerate all corporate IT networks and gain access to any network segment, even through VLAN security and firewalls were implemented on the network.
- Network Printer Causes 12 PLCs to Crash and Reboot
  - At a large manufacturing facility, several PLC devices were crashing and rebooting. The source of the packets was determined to be a network-connected printer that had ran out of ink and was sending out messages on all connected network segments. By the time they discovered the issue, these out-of-ink error messages had already crashed and rebooted 12 PLC devices on the plant floor.

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Over 60 different models of the LaserJet line alone have been launched since 1988.

Models [edit]

The model numbers do not necessarily have anything to do with the order of product development or the type of print-engine technology. For example, the LaserJet 1018 printer has newer, smaller, and more energy-efficient technology than the LaserJet 4000. The 1018 also features USB while the older 4000 does not.

Mono [edit]

- HP LaserJet Original Printer series
  - HP LaserJet Printer (March 1984)
  - HP LaserJet Plus Printer (November 1985)
  - HP LaserJet 500 Plus Printer (March 1986)
- HP LaserJet II Printer series (March 1987)
  - HP LaserJet Series II Printer
  - HP LaserJet IID Printer (1988)[7]
  - HP LaserJet IIp Printer (1989)
  - HP LaserJet IIp Plus Printer (1989)[7]
- HP LaserJet III Printer series (March 1990)
  - HP LaserJet III Printer (1990)[7]
  - HP LaserJet IIID Printer (1990)[7]
  - HP LaserJet IIIp Printer (1991)[7]
  - HP LaserJet IIISi Printer (March 1991)
- HP LaserJet 4 Printer series
  - HP LaserJet 4 (October 1992) / 4M Printer series
  - HP LaserJet 4 Plus / 4M Plus Printer series
  - HP LaserJet 4L / mL Printer series
  - HP LaserJet 4p / mp Printer series
  - HP LaserJet 4Si Printer series
  - HP LaserJet 4v / mv Printer series (1994)[7]
- HP LaserJet 5 Printer series
  - HP LaserJet 5 / m / n Printer series
  - HP LaserJet 5 (April 1996)
  - HP LaserJet 5L Printer series
  - HP LaserJet 5p / mp Printer series
  - HP LaserJet 5Si Printer series
- HP LaserJet 6 Printer series
  - HP LaserJet 6L Printer series
  - HP LaserJet 6L Pro Printer
  - HP LaserJet 6p/mp Printer series
- HP LaserJet 1000 Printer series
  - HP LaserJet 1000 Printer (2001)
  - HP LaserJet 1005 Printer
  - HP LaserJet 1010 Printer series
  - HP LaserJet 1012 Printer
  - HP LaserJet 1015 Printer
  - HP LaserJet 1018 Printer
  - HP LaserJet 1020 Printer series
  - HP LaserJet 1022 Printer series
  - HP LaserJet 1100 Printer series
  - HP LaserJet 1150 Printer
  - HP LaserJet 1160 Printer Series
  - HP LaserJet 1200 Printer series
  - HP LaserJet 1300 Printer series
  - HP LaserJet 1320 Printer series
- HP LaserJet 2000 Printer series (March 1987)
  - HP LaserJet 2000 Printer series
  - HP LaserJet 2100 Printer series (February 1999)[*citation needed*]
- HP LaserJet 2200 Printer series (2001)
  - HP LaserJet 2300 Printer series
  - HP LaserJet 2400 Printer series
- HP LaserJet 3000 Printer series (2006)
  - HP LaserJet 3100 Printer series
  - HP LaserJet 3200 Printer series
- HP LaserJet 4000 Printer series (1997)
  - HP LaserJet 4000 Printer series (1997)
  - HP LaserJet 4050 Printer series (1999)
  - HP LaserJet 4100 Printer series (2001)
  - HP LaserJet 4200 Printer series (2002)
  - HP LaserJet 4240n Printer
  - HP LaserJet 4250 Printer series
  - HP LaserJet 4300 Printer series
  - HP LaserJet 4350 Printer series
- HP LaserJet 5000 Printer series
  - HP LaserJet 5000 Printer series
  - HP LaserJet 5100 Printer series
  - HP LaserJet 5200 Printer series (2006)
- HP LaserJet 8000 Printer series (1998)
  - HP LaserJet 8000 Printer series
  - HP LaserJet 8100 Printer series
  - HP LaserJet 8150 Printer series (2004)
- HP LaserJet 9000 Printer series (2002)
  - HP LaserJet 9000 Printer series
  - HP LaserJet 9040 Printer series
  - HP LaserJet 9050 Printer series
- HP LaserJet P1500 Printer series
  - HP LaserJet P1505n Printer series
- HP LaserJet P2001 Printer series
  - HP LaserJet P2015 Printer series
- HP LaserJet P3000 Printer series (2006)
  - HP LaserJet Enterprise P3010 series (2009)
- HP LaserJet P4010 Printer series
- HP LaserJet P4500 Printer series
  - HP LaserJet P2035 (November 2013)
- ~~HP LaserJet Companion~~ *the LaserJet Companion is a sheet-fed monochrome scanner that connected to the parallel port of a LaserJet and provided copy functionality; as well as software scanning and fax functions.*

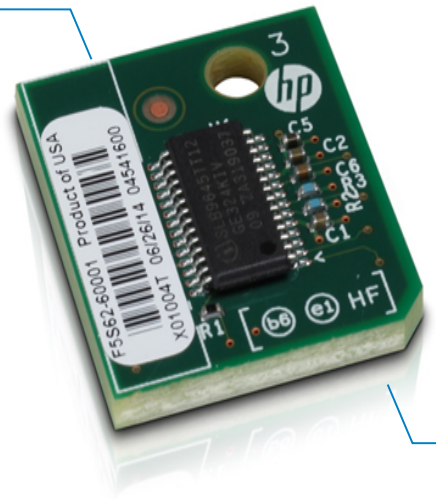
http://en.wikipedia.org/wiki/HP_LaserJet

HP Trusted Platform Module Accessory

Add an extra level of security safeguard to sensitive information

Highlights

Tamper-proof storage for key security credentials



HP Trusted Platform Module

Features

- Secures certificates, passwords and keys
- Simple install into existing systems
- Compatible with Enterprise MFP's and printers launched from Fall 2013 onward

© Copyright Red Tiger Security – Do not print or distribute without consent.

HP JetAdvantage Security Portfolio

Network Security

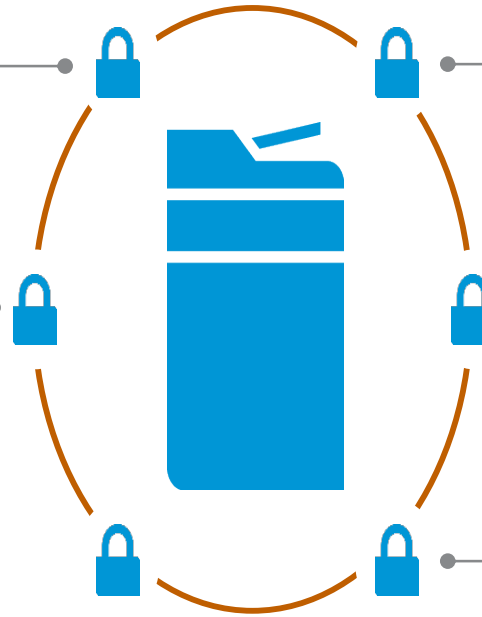
- Secure communication to/from the device
- Firewall
- Certificates

Data Protection

- Encrypted storage w/secure erase
- Secure print / secure mobile print
- Secure capture
- HP Secure Content Monitoring & Management

Monitoring and Management

- HP Imaging & Printing Security Center
- HP Security Advisory Services
- HP ArcSight (SIEM) Printer Integration
- HP FutureSmart firmware updates
- HP Access Control: Job Accounting



Content Security

- HP Access Control: Secure Pull Printing
- HP JetAdvantage Pull Print
- HP UPD Secure Encrypted Print
- HP & Troy Document Protection

Access Controls

- PIN, LDAP, Kerberos
- Role-based access control
- HP Access Control: Secure Authentication
- HP SmartCard Solutions for US Gov't

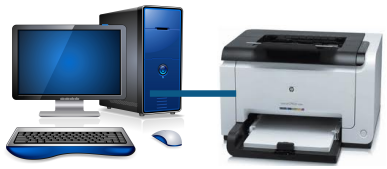
Device Security

- Admin access controls
- Physical security (locks, port disablement)
- Common Criteria Certification
- HP Trusted Platform Module

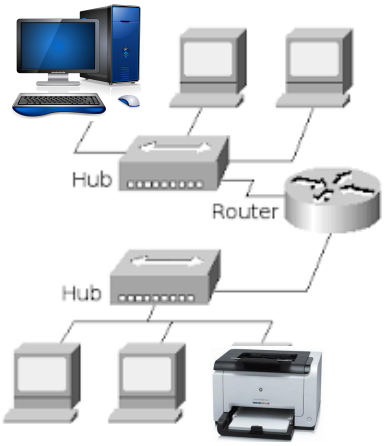
© Copyright Red Tiger Security – Do not print or distribute without consent.

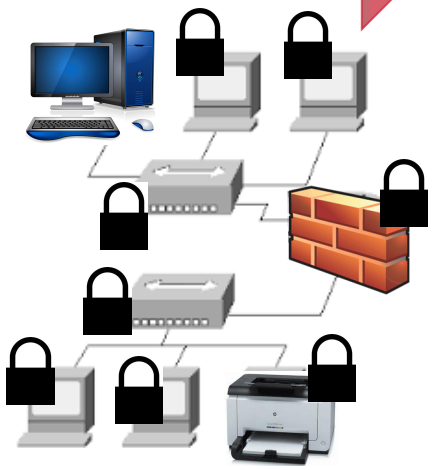
Printers have a similar evolution path as ICS embedded devices

Serial / RS-232 → **Bus / Token Ring** → **1st Gen TCP/IP** → **Secure TCP/IP**

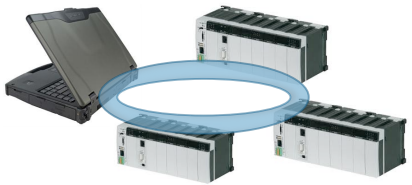


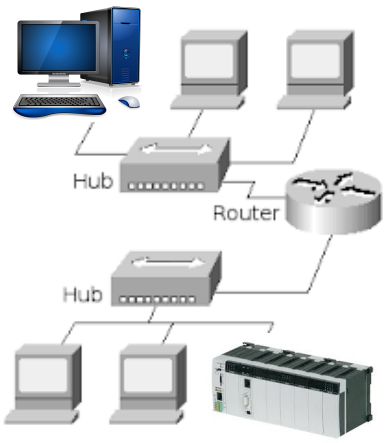














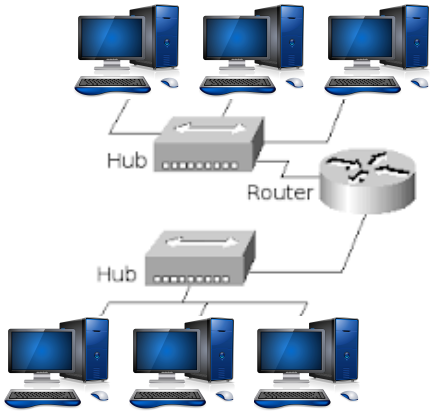
© Copyright Red Tiger Security – Do not print or distribute without consent.

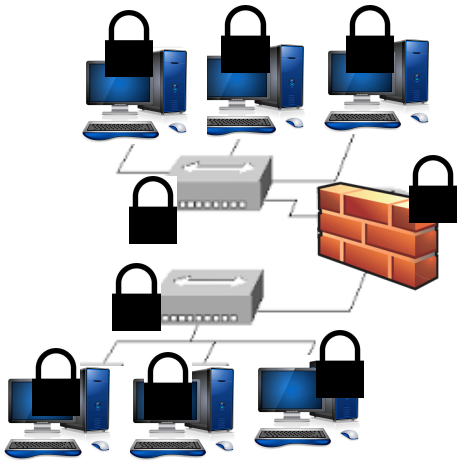
Printers and Embedded Devices Left Behind in Security Evolution

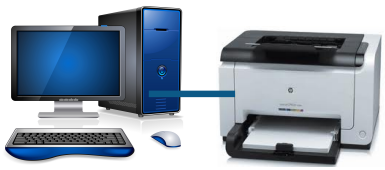
Serial / RS-232 → **Bus / Token Ring** → **1st Gen TCP/IP** → **Secure TCP/IP**



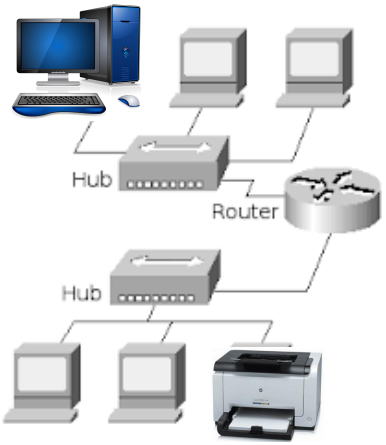


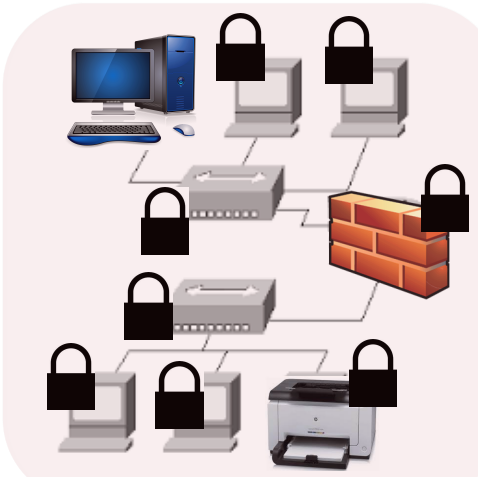












© Copyright Red Tiger Security – Do not print or distribute without consent.

Lessons Learned

- **Embedded IT devices** have been able to embed security features into devices along with their technology evolution, unlike ICS embedded devices that remain largely unchanged since the RS-232 days
- HP recognized that their embedded devices lacked the same security features that their servers, computers, laptops, network devices and mobile devices offered and made a **strategic decision** to correct this.
- Designing a common security framework that would be able to be backward compatible with over 60 models of printers with various hardware implementations was not easy, and in the end the team decided to focus on **cross-capabilities for all printers made after 2014**.

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

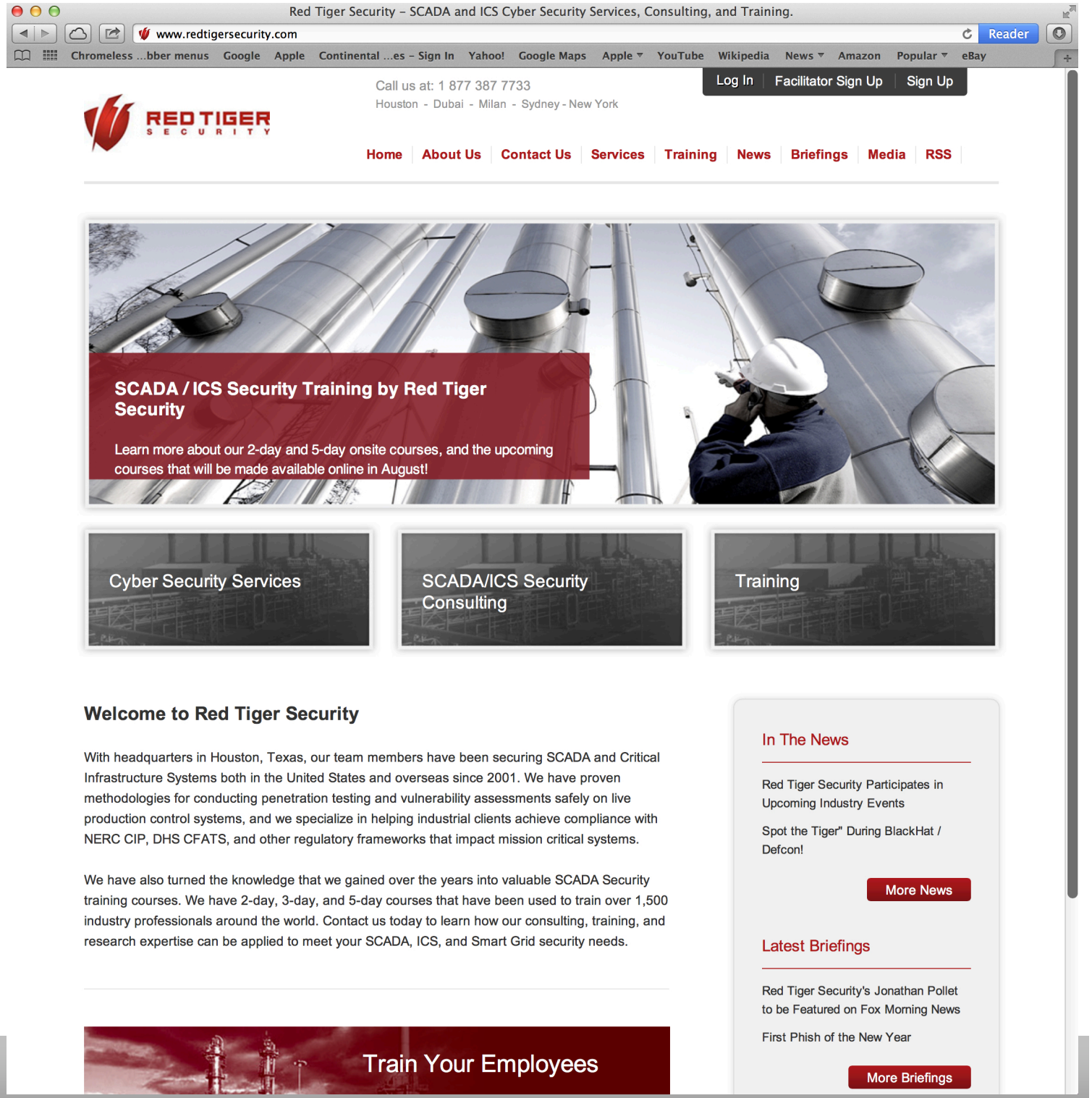
Lessons Learned

- Design decision included an external chipset to handle many of these additional security features
- Ability to **manage the security of a large fleet of devices** was another major design theme
- **They did not charge customers for these new security features**
- All security features now part of every printer shipped
- HP chose to invest in security to be a **market leader**…others will follow
- Entire process took 2 years, and ICS vendors serious about security can take a similar approach
- **NO MORE EXCUSES!**

© Copyright Red Tiger Security – Do not print or distribute without consent.

RED TIGER SECURITY

Get More Training and Awareness



web: redtigersecurity.com



Contact Information:

Jonathan Pollet, CAP, CISSP, PCIP

Founder, Executive Director

Red Tiger Security

Mobile: +1.281.748.6401

Email: jpollet@redtigersecurity.com

Twitter: @jonpollet

Follow and link to us for industry updates and briefings:

www.redtigersecurity.com

www.twitter.com/redtigersec

www.facebook.com/redtigersec

www.linkedin.com/company/red-tiger-security