

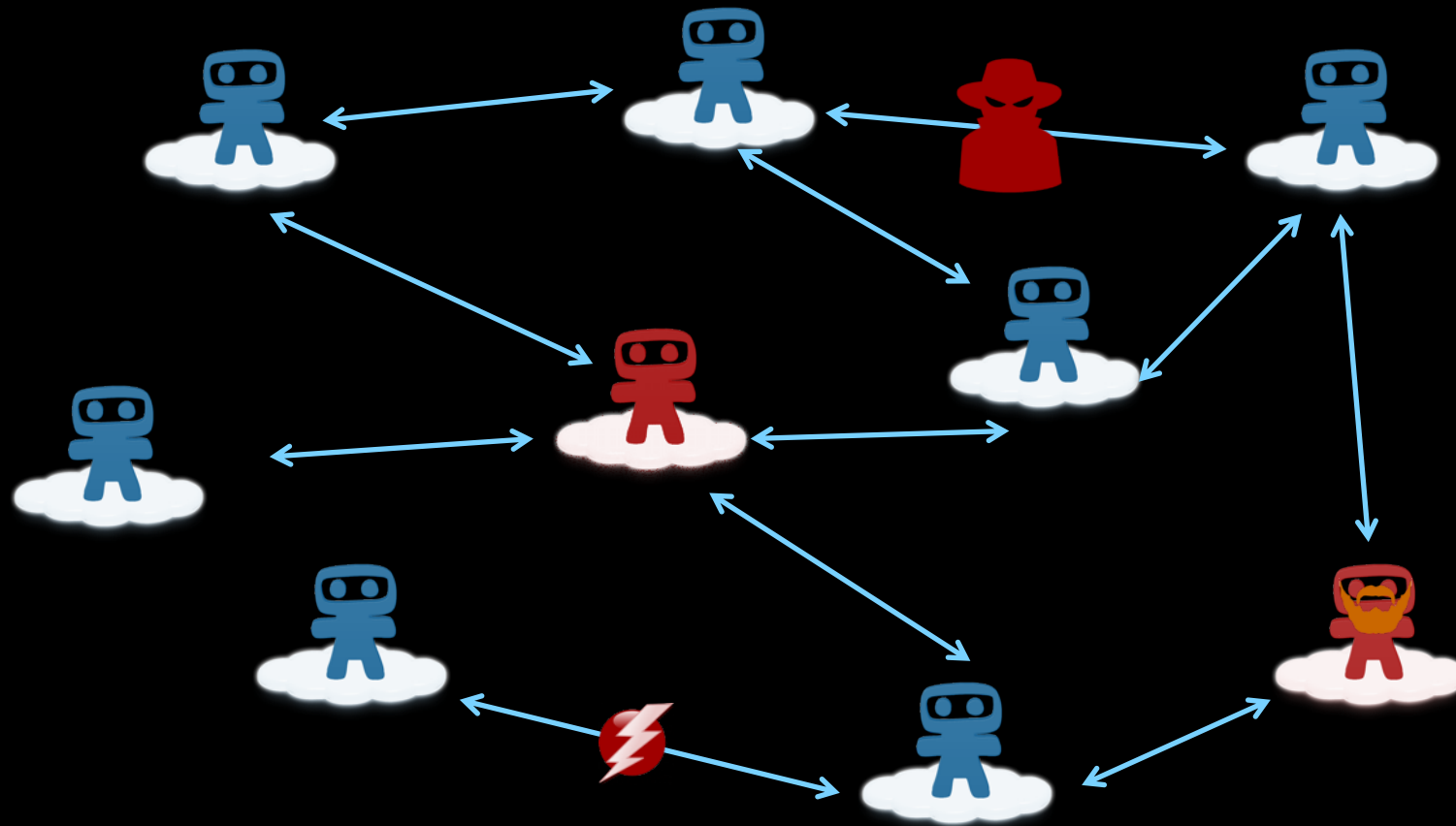
IoT: Attack of the Clone Army?

Dr Ralf Huuck

London, December 2016



Some IoT Threat Vectors



Man-In-The-Middle
between machines

Faulty Device

Faulty Connection

Outdated Software/
Default Passwords

Hack One – Control All

Billions of IoT devices in the near future.

Each IoT Product million times the same.

One Breach = One Clone Army.



BreakingNews



Breaking Old News



briankrebs @briankrebs · Sep 21

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. [#FAIL](#)



867



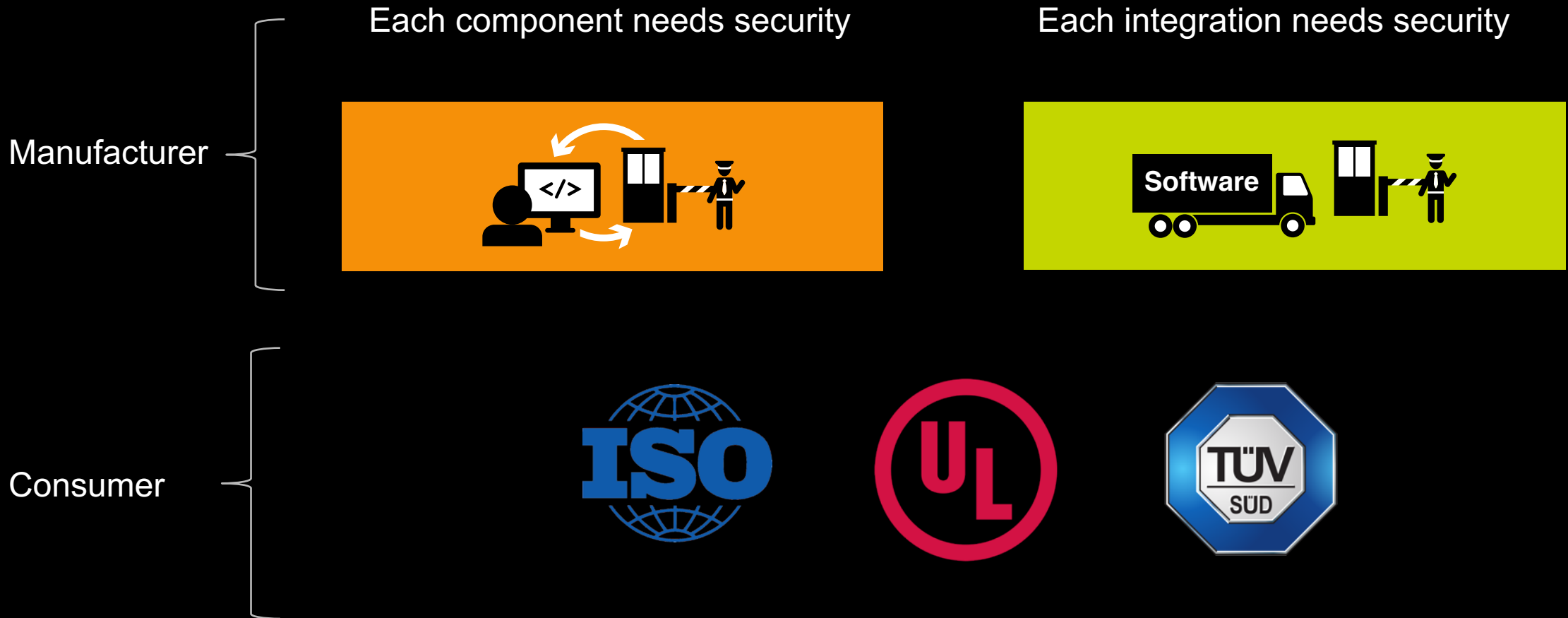
1.2K



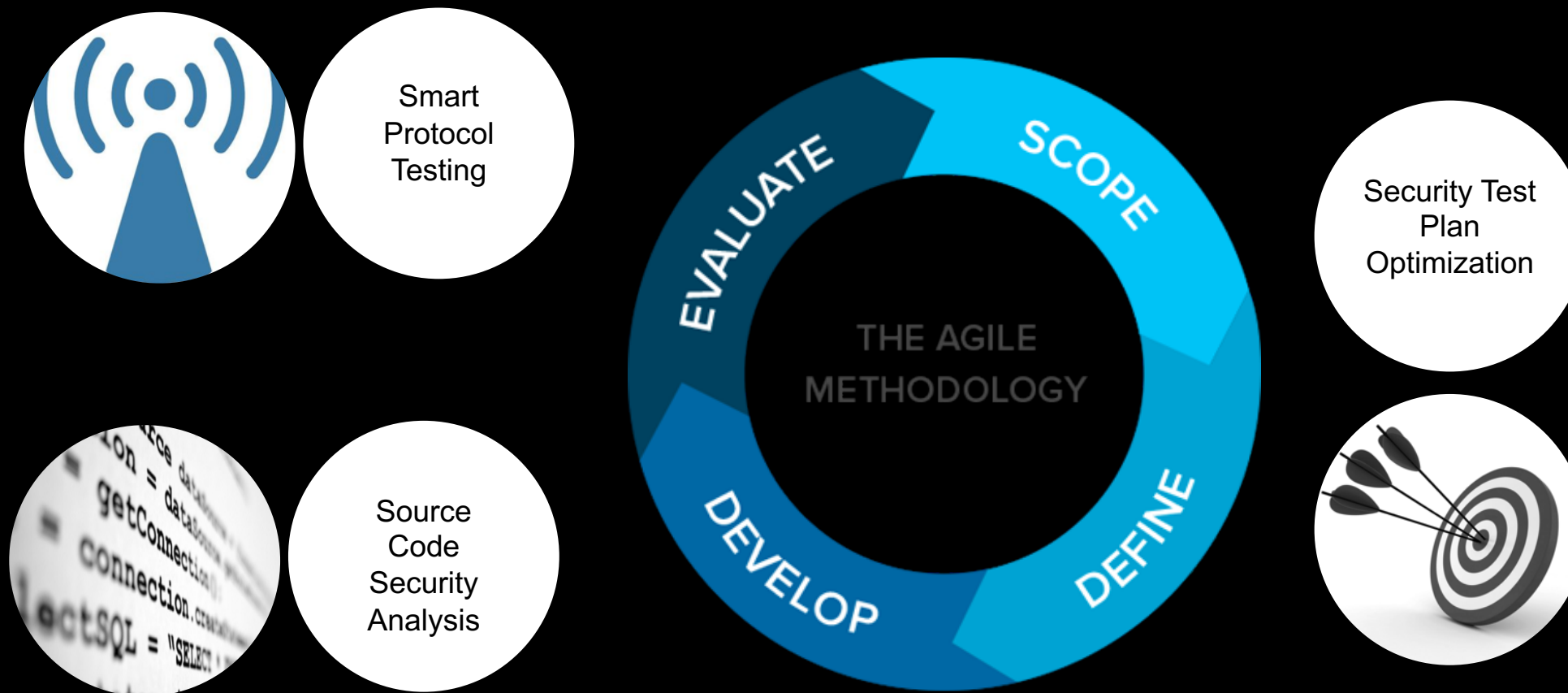
145,607 hacked digital video recorders and IP cameras.

Where to Go From Here?

Prevention from the Ground Up



Securing Software Lifecycle: Automation



Example: Protocol Fuzzing

Protocols

Software systems and components communicate

Automated Malformed Input Testing

Finding unknown, exploitable vulnerabilities

Hacking Preventions

Patch holes before exploitation

Core Internet	Net Management	Routing
IPv4 (TCP, UDP, ICMP, IGMP, ARP), IPv6 (TCP, UDP, ICMPv6), IPsec, DNS, DNS-SEC, NTP (Client, Server), DHCP/BOOTP Client, DHCP/BOOTP Server, HTTP Server, HTTP Client, FTP Server, DHCPv6 Client, DHCPv6 Server, MIPv6 (Client, Server)	HTTP Server, HTTP Client, TLS/SSL Server, TLS/SSL Client, Telnet Server, SSH1 Server, SSH2 Server, SNMPv1/v2 Server, SNMPv3 Server, TFTP Server, UPnP Server, Syslog, SNMP TRAP	IS-IS, DVMRP, GRE, OSPFv2, OSPFv3, PIM-SM/DM, RSVP, VRRP, BGP4, RIP, RIPng, MPLS/LDP, HSRP, NHRP

Remote Access	VPN	VoIP/IMS
EAPOL Server, PPPoE, Diameter Server, Diameter Client, LDAPv3 Server, TACACS+ Server, TACACS+ NAS, RADIUS (Server, Client), Kerberos Server	IPSec, SSH1 Server, SSH2 Server, TLS/SSL Server, TLS/SSL Client, ISAKMP/IKEv1 (Client, Server), IKEv2, OCSF (Client, Server), L2TPv2, L2TPv3, x.509	SCTP, H.248, H.323, RTSP (Client, Server), TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, SigComp, RTP/RTCP/SRTP, MGCP, UPnP Server, SMP, x.509, BICC, STUN, TURN, Diameter

3G / 4G-LTE	Digital Media	Email
SCTP, GRE, IPsec, Diameter (Server, Client), LDAP Server, TLS/SSL (Server, Client), SIP UAS, SIP UAC, GTPv0, GTPv1, GTPv2, RADIUS (Server, Client), PMIP	AIFF, AU, AMR, IMY, MP3, VOC, WAV, BMP, GIF, JPEG, MBM, PCX, PNG, PIX, PNM, RAS, TIFF, WBMP, XBM, XPM, WMF, AVI, Quicktime, MPG1, MPG2, MPEG4, ZIP, CAB, JAR, LHA, GZIP, vCalendar, VCard	POP3 Client, POP3 Server, IMAP4 Client, IMAP4 Server, SMTP Client, SMTP Server, MIME

File Systems/Storage	WLAN	Link Management
CIFS/SMB Server, iSCSI Server, SunRPC Server, NFS Server, SMBv2, FCoE, FIP, PFC	802.11 Server, 802.11 Client, WPA Server, WPA Client	LACP, STP, MSTP, RSTP, ESTP

Bluetooth	IPTV	PDA/ Smartphone
L2CAP, SDP, RFCOMM, OBEX, OPP, FTP, IrMC Sync, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP, HFP Client, HSP Client, BPP, MDP/HDP, 2.1 compliant	MPEG4, MPEG2, IPsec, TLS/SSL, RTP/RTCP, RTSP, HTTP, FTP, TFTP, IPv4, PIM-SM/DM, RSVP, IGMP, CWMP (TR-69), MPEG2-TS, SIP-UAS, SIP-UAC	IPv4, DHCP/BOOTP, HTTP, TLS/SSL, UPnP, SIP, Audio, Images, Video, Bluetooth, 802.11

Industrial Automation	Archives	Metro Ethernet
(SCADA/DCS) Modbus, IPv4 (TCP, UDP, ICMP, IGMP, ARP)	GAB, GZIP, JAR, LHA, ZIP	BFD, CFM, E-LMI, Ethernet, GARP, LLD, OAM, PBT/PBB-TE, STP/RSTP/MSTP/ESTP, PTP, SyncEthernet

Example: Static Code Analysis



XSS, Injections, CSRF,
Security vulnerabilities



Memory violations,
Logic errors, Defects



Race conditions, Memory corruption,
Concurrency errors, Deadlocks

automated scan during coding

CID	Type	Component	Impact	Status	Count	First Detected	Owner	Classification	Severity	Action	Component
42005	SQL Injection	webgoat.Other	Absent	High	New	1	09/09/12	Unassigned	Unspecified	Undesired	webgoat.Other
42004	SQL Injection	webgoat.Other	Absent	High	New	1	09/09/12	Unassigned	Unspecified	Undesired	webgoat.Other
42003	SQL Injection	webgoat.Other	Absent	High	New	2	09/09/12	Unassigned	Unspecified	Undesired	webgoat.Other
42002	SQL Injection	webgoat.Other	Absent	High	New	1	09/09/12	Unassigned	Unspecified	Undesired	webgoat.Other
42001	SQL Injection	webgoat.Other	Absent	High	New	1	09/09/12	Unassigned	Unspecified	Undesired	webgoat.Other
38346	SQL Injection	psiprobe.Other	Absent	Medium	Triaged	1	06/01/12	jon	Pending	Unspecified	psiprobe.Other

1 of 57 issues selected

BackDoors.java

```
protected Element concept2(WebSession s) throws Exception
{
    ElementContainer ec = new ElementContainer();
    ec.addElement(nakUsername(s));

    5 taint_path_call: org.owasp.webgoat.session.ParameterParser.getRawParameter(java.lang.String, java.lang.String) returns the tainted data.
    String userInput = s.getParameter().getRawParameter(USERNAME, "");
    if (!userInput.equals(""))
    {
        CID 42004 (#1 of 1): SQL Injection (SQL)
        6 sql_taint: Insecure concatenation of a SQL statement. The value userInput is tainted.
        Remediation for SQL injection in JDBC: Specific advice for SQL data value
        - Refactor the JDBC code to use the PreparedStatement API versus Statement.
        - Add a positional parameter to the SQL statement using "?".
        - Bind the tainted value to the parameter using the setString method: PreparedStatement.setString(1, userInput).
        More Information:
        userInput = SELECT_ST + userInput;
        String[] arrSQL = userInput.split(":");
        Connection conn = DatabaseUtilities.getConnection(s);
        Statement statement = conn.createStatement(ResultSet.TYPE_SCROLL_INSENSITIVE, ResultSet.CONCUR_READ_ONLY);

        if (arrSQL.length == 2)
        {
            if (userInput.toUpperCase().indexOf("CREATE TRIGGER") != -1)
            {
                makeSuccess(s);
            }
        }

        7 sql_sink: Passing the tainted value arrSQL[0] to the SQL API java.sql.Statement.executeQuery(java.lang.String) may allow an attacker to inject SQL.
        ResultSet rs = statement.executeQuery(arrSQL[0]);
        addDBEntriesToEC(ec, rs);

        CID 41918: Resource leak (RESOURCE_LEAK) [select issue]
    }
    return ec;
}
```

42004 SQL Injection

A user can change the intent of the SQL query, which may inappropriately disclose or corrupt data within the database. In org.owasp.webgoat.session.BackDoors.concept2(s): org.owasp.webgoat.session.WebSession: Untrusted user-supplied data is inserted into a SQL statement without adequate validation, escaping, or filtering (CWE-89)

Classification: Bug
Severity: Moderate
Action: Fix Required
Ext. Reference: Type attribute text
Confidence: High
MISRA Status: Not applicable
Owner: Billy (Billy)

Enter comments (See the Triage History section below for previous comments)

Apply + Next Apply

Projects & Streams
Detection History
Triage History
Occurrences

1: webgoat

Events contributing to issue:

Data flow from tainted source to query construction

#	Tainted Source	Parameter
1	tainted_source	ParameterParser.java:5
2	taint_path_return	ParameterParser.java:5
3	taint_path_call	ParameterParser.java:4
4	taint_path_return	ParameterParser.java:4
5	taint_path_call	BackDoors.java:168
6	sql_taint	BackDoors.java:168
7	sql_sink	BackDoors.java:180

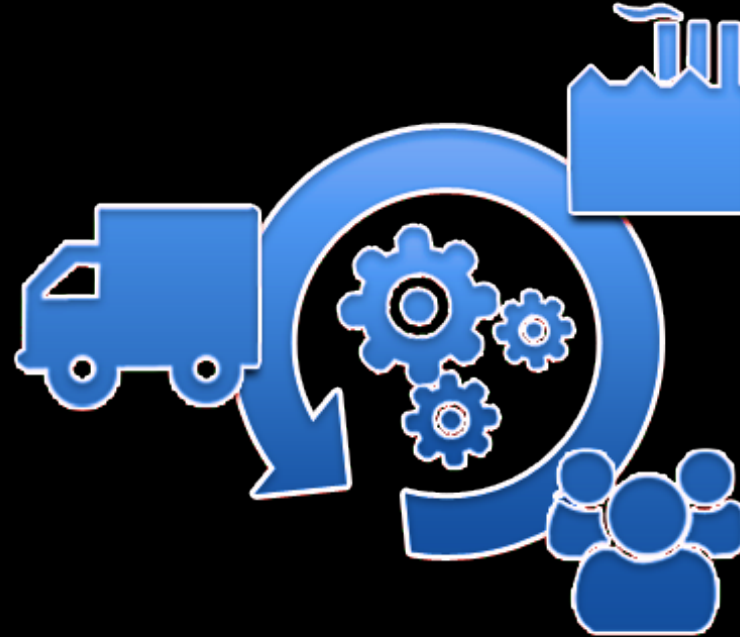
Securing Software Supply Chain: Automation



Smart
Protocol
Testing



Software
Composition
Analysis



Runtime
Security
Analysis



Example: 3rd Party Component Scanning

NIST

Daily updates from National
Vulnerability Database (NVD)

THOUSANDS
of binary
component signatures

HUNDREDS of
THOUSANDS
of open source
projects data base

Component information

Name	libpng
Version	1.5.10 Change
Latest version	1.6.18 OUTDATED
License	libpng PERMISSIVE
Website	www.libpng.org
Tags	IMAGE

COVERITY SCAN [Scan Dashboard](#)

This open source project has registered their product with Coverity Scan for finding source code defects and vulnerabilities.

Last analysed in Scan: about a month ago

Defect density: low (0)
Defect density is low compared to an average of 0.7 in other projects that are similar in size.
[Show defect density over time](#)

Objects with this component

Timestamp	File
2015-04-29 11:00:25	4.hfs:/F-Secure Freedom/Freed... meworks/QtGui.framework/Versions/5/QtGui

Known vulnerabilities (CVSS ranges: 0-3.9 minor, 4.0-6.9 major and 7.0-10.0 critical)

CVE	Date	CVSS	Type
CVE-2014-9495	2015-01-10	10	Exact match
CVE-2015-0973	2015-01-18	7.5	Exact match
CVE-2011-3048	2012-05-29	6.8	Exact match
CVE-2013-7353	2014-05-06	5	Exact match

Example: Runtime Monitoring

Live tracking of data.

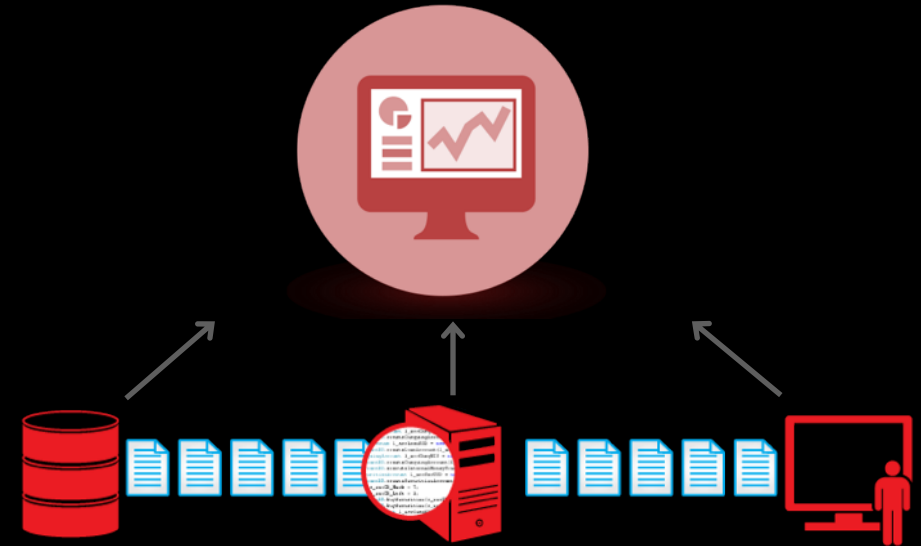
Analyzes code as it runs, line by line

Tracks data throughout the application

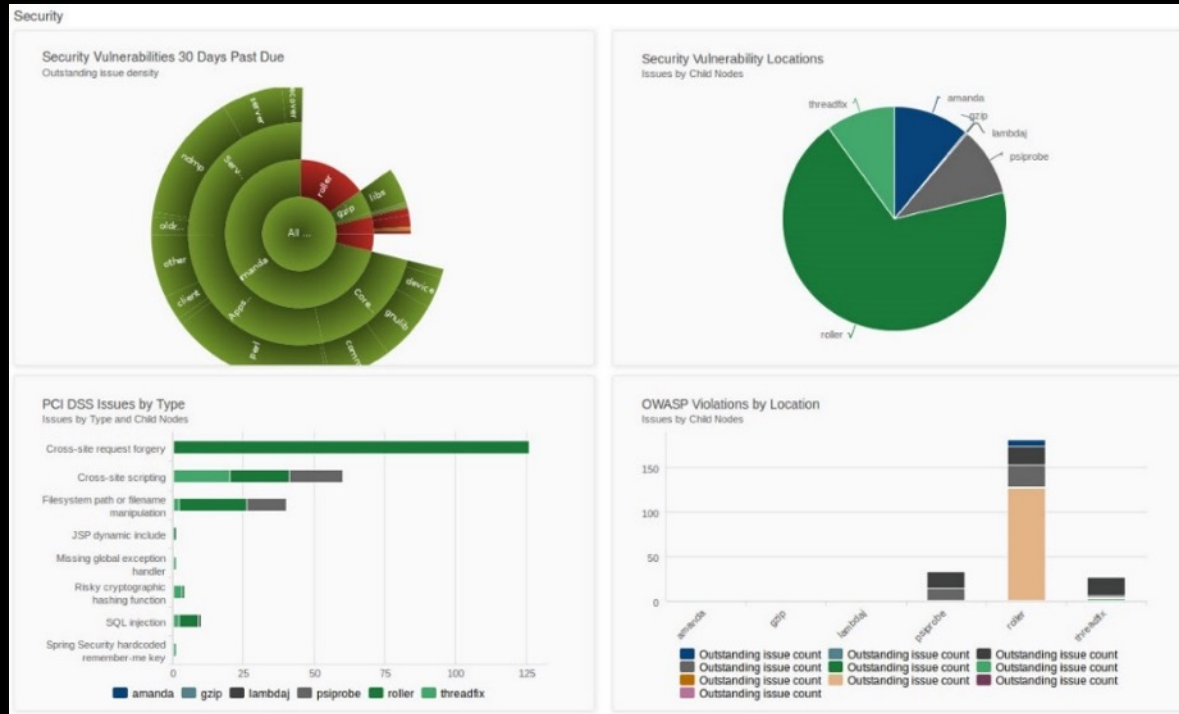
Maps business processes in the application

Simulates attacks (exploits)

Integrate with test systems.



Automated DevOps Security: Real-time View



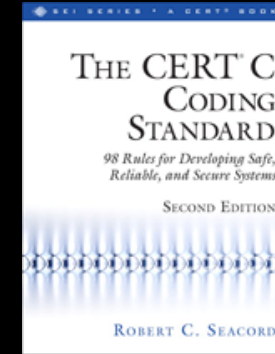
Independent Security Authorities



IoT Cyber
Security
Assurance



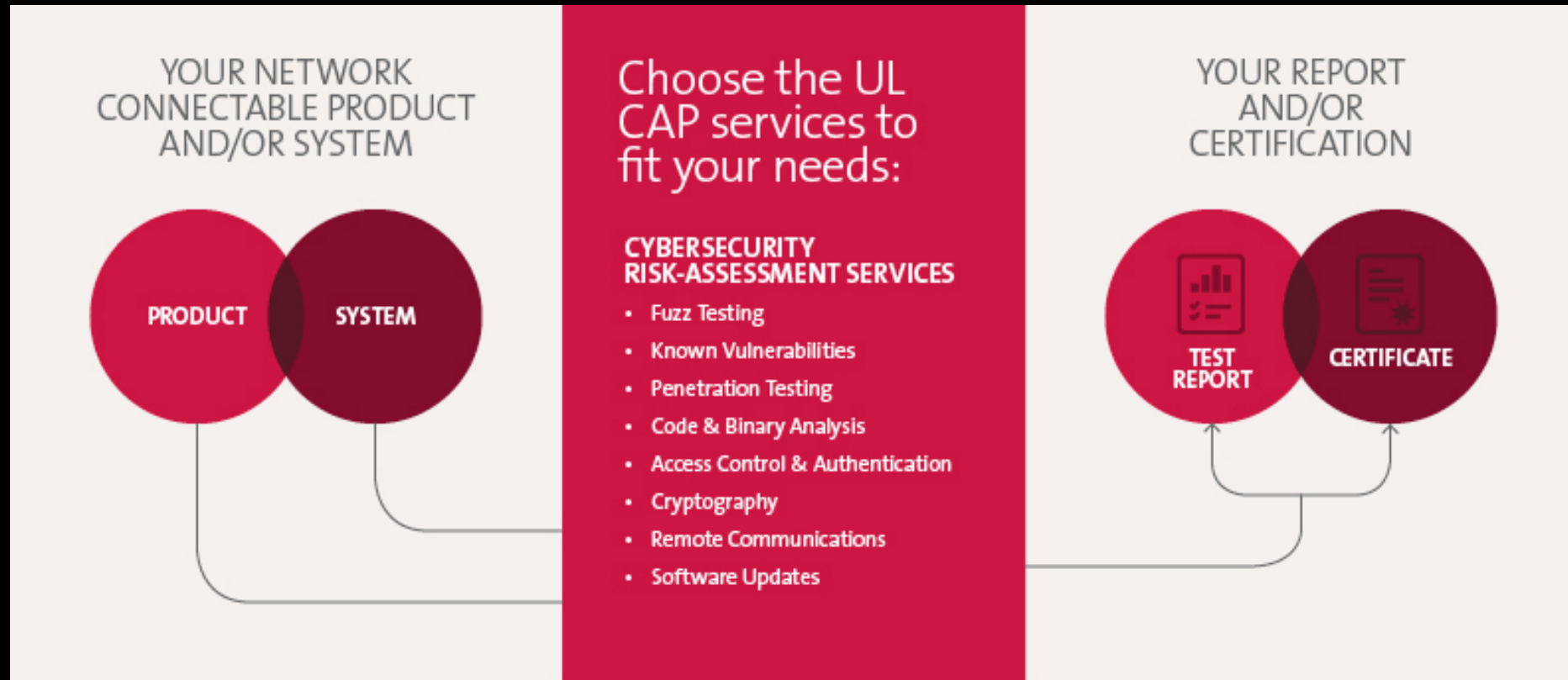
Secure
Software
Dev



Cyber
Security
Insurance



Example: UL 2900 Cybersecurity Assurance Program



Assessment with time-bounded certification horizon.

Summary

Challenges Are Not Getting Smaller.

75-300 billion networked devices by 2022

– David Bray, CIO FCC

Cybercrime costs \$3 trillion to economy

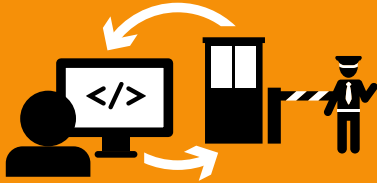
– World Economy Forum

Security pros think over 50% of IoT products are insecure

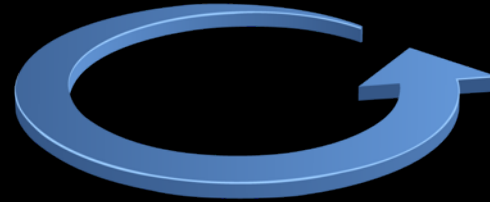
– IOActive

No Single Responsibility

Signoff for Software Development



Signoff for Supply Chain



Signoff for Consumer Confidence



Future Challenges

How to Stop Breaches from Spreading?

Legal & Technical Constraints?



CONTAINMENT

Shutting Down Rogues IoT Systems?

Geopolitical Implication?

Contact



Dr Ralf Huuck
Synopsys
ralf.huuck@synopsys.com

Q&A

