The Need for Confluence

The Essential Role of Incident Response in Secure Software Development

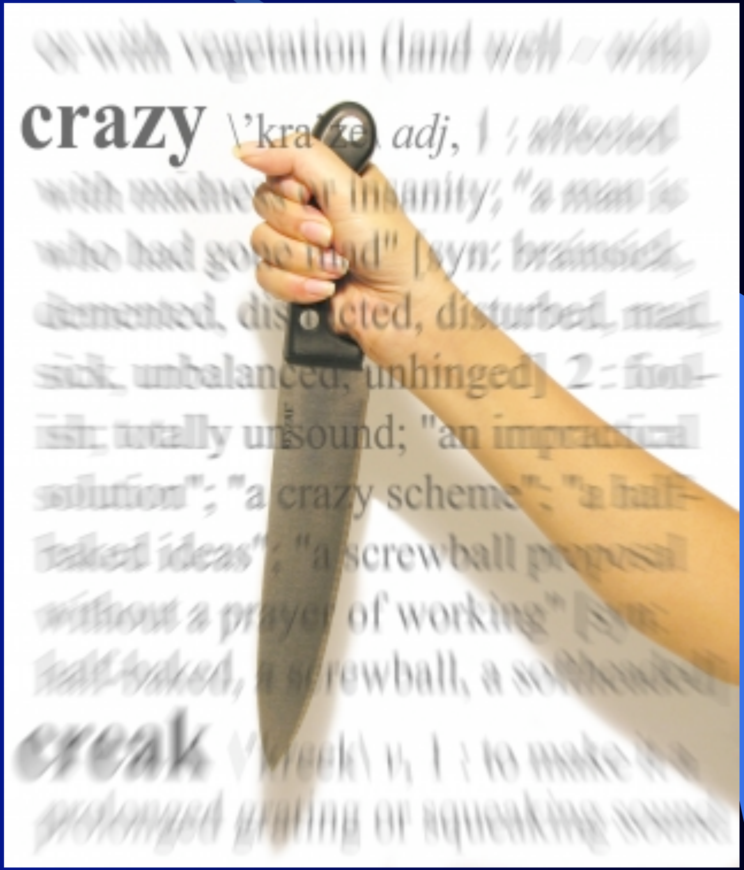
Why do security incidents occur?

What is the root cause?

Faulty software (more often than not)

What is the definition of insanity?

- Year after year
- Thousands upon thousands of incidents
- Same root cause
- What are we doing about it?
- We *talk* about proactive, but do we do it? *Really*?



You can’t bolt security on later

- A room full of firewalls, intrusion detection|prevention systems, etc., will not protect bad software
- We must address the root causes
- Active participation in development

Why aren’t things improving?

Learn from history

- We don’t pay enough attention to our failures
- Consider other engineering disciplines

Lack of knowledge

- Developers tend to not have security knowledge
- Security team tends to not have development knowledge
- “Us” and “them”

We’re overly trusting

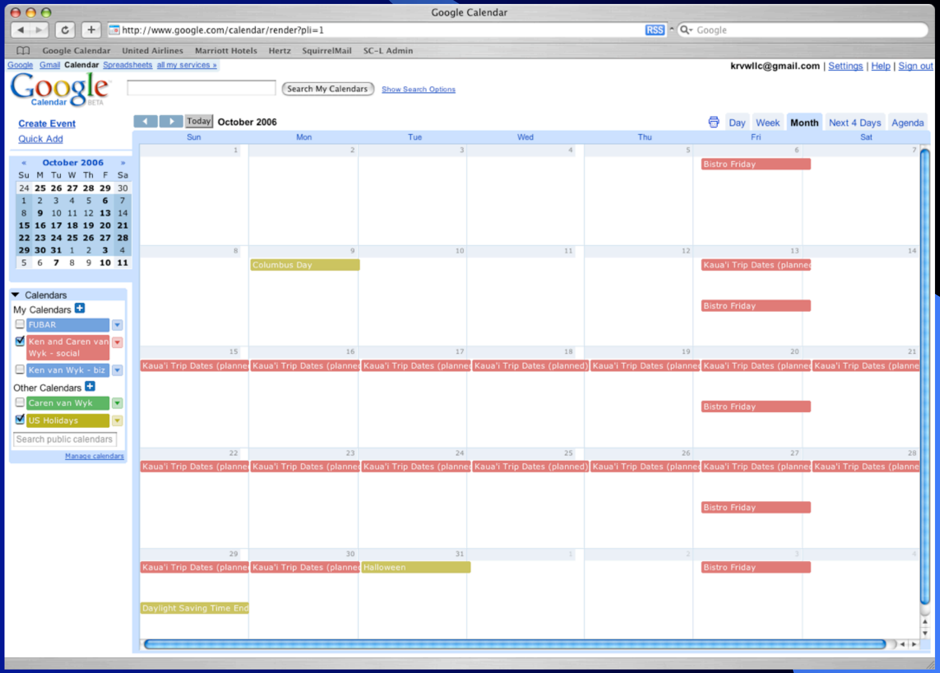
- We tend to have misplaced trust in our users
- Sometimes users are malicious
- Sometimes they don’t even try to be

Focus

- Too much attention is paid to functional spec
- Consider what can go wrong as well

Complexity

- Complexity is fighting us every step of the way
- Consider AJAX


Google Calendar
http://www.google.com/calendar/render?pli=1
RSS
Google
Google Calendar United Airlines Marriott Hotels Hertz SquirrelMail SC-L Admin
Google Gmail Calendar Spreadsheets all my services »
krvwllc@gmail.com | Settings | Help | Sign out
Google Calendar BETA
Search My Calendars
Show Search Options
Create Event
Quick Add
Today
Day
Week
Month
Next 4 Days
Agenda
Calendars
My Calendars
Other Calendars
Search public calendars
Manage calendars

☐ FUBAR
☑ Ken and Caren van Wyk - social
☐ Ken van Wyk - biz
☐ Caren van Wyk
☑ US Holidays

« October 2006 »

Su	M	Tu	W	Th	F	Sa
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

October 2006

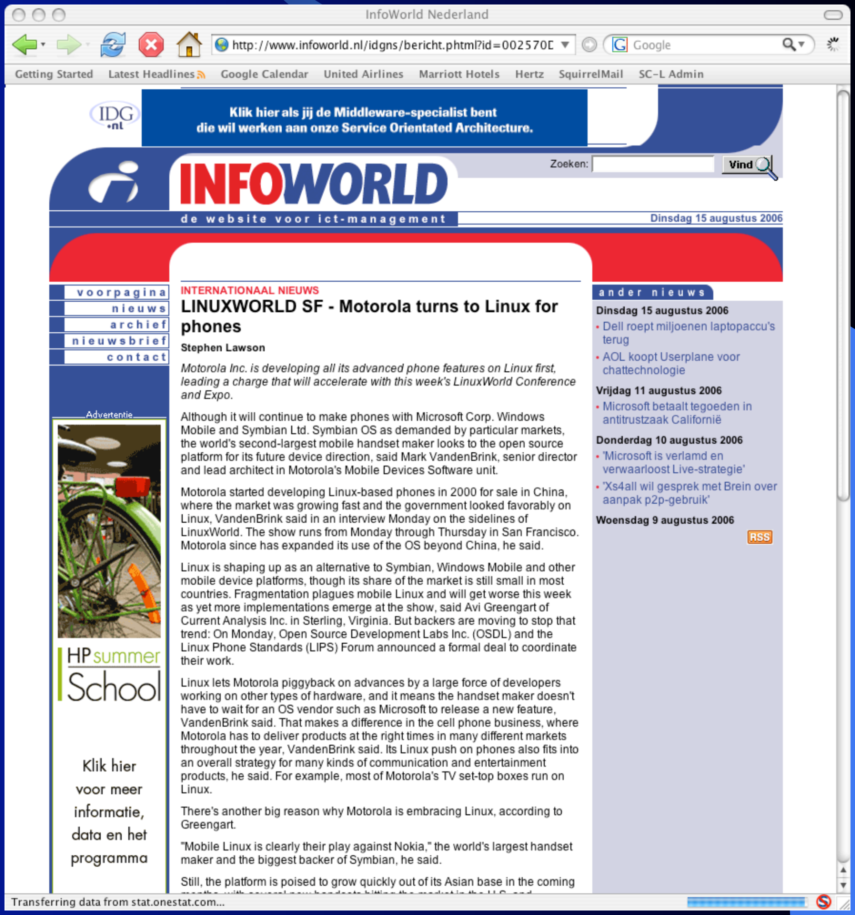
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6 Bistro Friday	7
8	9 Columbus Day	10	11	12	13 Kaua'i Trip Dates (planne Bistro Friday	14
15 Kaua'i Trip Dates (planne	16 Kaua'i Trip Dates (planne	17 Kaua'i Trip Dates (planne	18 Kaua'i Trip Dates (planned)	19 Kaua'i Trip Dates (planne	20 Kaua'i Trip Dates (planne Bistro Friday	21 Kaua'i Trip Dates (planne
22 Kaua'i Trip Dates (planne	23 Kaua'i Trip Dates (planne	24 Kaua'i Trip Dates (planne	25 Kaua'i Trip Dates (planned)	26 Kaua'i Trip Dates (planne	27 Kaua'i Trip Dates (planne Bistro Friday	28 Kaua'i Trip Dates (planne
29 Kaua'i Trip Dates (planne Daylight Saving Time End	30 Kaua'i Trip Dates (planne	31 Halloween	1	2	3 Bistro Friday	4

Connectivity

- Connectivity is everywhere
- Do you know where your data is?
- Consider mobile users, SOAP, grid computing

Extensibility

- Extensibility isn’t what it used to be
- Who wants a computer that isn’t?
- Is your desktop user privileged?


InfoWorld Nederland
http://www.infoworld.nl/idgns/bericht.phtml?id=002570D
Google
Getting Started Latest Headlines Google Calendar United Airlines Marriott Hotels Hertz SquirrelMail SC-L Admin
IDG .nl
Klik hier als jij de Middleware-specialist bent die wil werken aan onze Service Orientated Architecture.
Zoeken:
Vind
INFOWORLD
de website voor ict-management
Dinsdag 15 augustus 2006
voorpagina
nieuws
archief
nieuwsbrief
contact
Advertentie
HP summer School
Klik hier voor meer informatie, data en het programma
Transferring data from stat.onestat.com...

INTERNATIONAAL NIEUWS

LINUXWORLD SF - Motorola turns to Linux for phones

Stephen Lawson

Motorola Inc. is developing all its advanced phone features on Linux first, leading a charge that will accelerate with this week's LinuxWorld Conference and Expo.

Although it will continue to make phones with Microsoft Corp. Windows Mobile and Symbian Ltd. Symbian OS as demanded by particular markets, the world's second-largest mobile handset maker looks to the open source platform for its future device direction, said Mark VandenBrink, senior director and lead architect in Motorola's Mobile Devices Software unit.

Motorola started developing Linux-based phones in 2000 for sale in China, where the market was growing fast and the government looked favorably on Linux, VandenBrink said in an interview Monday on the sidelines of LinuxWorld. The show runs from Monday through Thursday in San Francisco. Motorola since has expanded its use of the OS beyond China, he said.

Linux is shaping up as an alternative to Symbian, Windows Mobile and other mobile device platforms, though its share of the market is still small in most countries. Fragmentation plagues mobile Linux and will get worse this week as yet more implementations emerge at the show, said Avi Greengart of Current Analysis Inc. in Sterling, Virginia. But backers are moving to stop that trend: On Monday, Open Source Development Labs Inc. (OSDL) and the Linux Phone Standards (LIPS) Forum announced a formal deal to coordinate their work.

Linux lets Motorola piggyback on advances by a large force of developers working on other types of hardware, and it means the handset maker doesn't have to wait for an OS vendor such as Microsoft to release a new feature, VandenBrink said. That makes a difference in the cell phone business, where Motorola has to deliver products at the right times in many different markets throughout the year, VandenBrink said. Its Linux push on phones also fits into an overall strategy for many kinds of communication and entertainment products, he said. For example, most of Motorola's TV set-top boxes run on Linux.

There's another big reason why Motorola is embracing Linux, according to Greengart.

"Mobile Linux is clearly their play against Nokia," the world's largest handset maker and the biggest backer of Symbian, he said.

Still, the platform is poised to grow quickly out of its Asian base in the coming

ander nieuws

Dinsdag 15 augustus 2006
- Dell roept miljoenen laptopaccu's terug
- AOL koopt Userplane voor chattechnologie

Vrijdag 11 augustus 2006
- Microsoft betaalt tegoeden in antitrustzaak Californië

Donderdag 10 augustus 2006
- 'Microsoft is verlamd en verwaarloost Live-strategie'
- 'Xs4all wil gesprek met Brein over aanpak p2p-gebruik'

Woensdag 9 augustus 2006

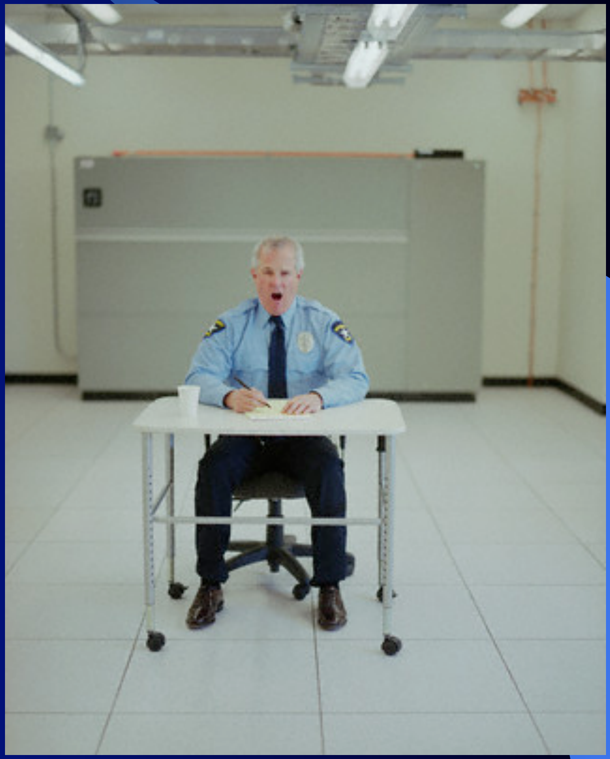
RSS

Old school paradigms

- Old school information security solutions don’t adequately protect the *software*
- Consider IM, Skype, WiFi, VPNs

Testing isn't working

- Software testing does not adequately address security
- Penetration testing is not sufficient



So how can we help?

- Deep integration into the development process
- Consider five stages
  - Requirements
  - Design
  - Code
  - Testing
  - Deployment

But first, think positive

- We're too quick to use negative models
  - Anti-virus products
  - Signature-based IDS
  - Vulnerability scanning
- These are not adequate
  - Think positive validation
- Prove something safe and then allow it
  - All else is evil
- Throughout a system
  - From OS through application
- Prime example
  - Input validation

Part of the team

- Don't just be a reviewer/auditor
  - Adversarial role can be detrimental
- Be a security consultant to dev
  - Each project
  - Guide and assist the dev team

Requirements

- Help build security requirements
  - Regulatory compliance
  - Abuse/misuse cases
- Guide discussions on what bad things can happen
- Focus on lessons learned
  - Cite similar architectures and failures
- Requirements must be actionable
  - Focus on "must not" actionable statements

Design

- Help conduct design reviews
- Consider available approaches
  - Microsoft's threat modeling
  - Cigital's ARA
- Identify and prioritize design weaknesses
  - Based on business risk
- Build mitigations for high priority risks
- Nightmare scenarios can be useful

Code

- Learn the technologies
- Help build prescriptive language guidance
  - Input validation
  - SQL utilization
  - Authentication
  - Session management
- Help build reusable class libraries frameworks
  - Enterprise coding standards
- Code reviews to verify compliance
  - Manual vs. automated
- Look at open projects
  - OWASP’s ESAPI

Testing

- Penetration testing alone is not enough
  - Coverage
  - Internals
- Consider Microsoft's testing approach
  - Fuzzing
  - Pen testing
  - Dynamic validation
- Results must be meaningful to the dev team
  - Findings by code module
  - Integrate with bug tracking s/w
  - Prescriptive guidance

Deployment

- Verification of safe deployment environment
  - Not just pen testing
  - Host hardening
  - File access controls
  - Event monitoring
- Verify and validate manually and empirically
  - Time to break out the network sniffer
- If WAFs used, help train the WAF on app’s normative behavior

Issues to consider

- Cultural barriers
  - Years of "us and them" may be tough to overcome
  - Developers "allergic" to security
  - Authority to mandate
  - Positive incentive
- Consider small steps towards a goal
  - But first, understand what the goal is
- Measurement helps
  - Track and show improvement

Checklist of things to do

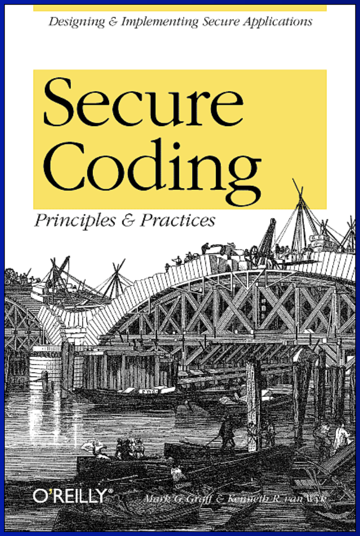
- Read, study, learn
  - Work through OWASP WebGoat exercises
  - Language references
  - See reference list
- Seek dev team
  - Discuss possible roles and responsibilities
- Learn dev environment
  - Bug tracking
  - Process
- Pilot studies
  - Pick a project and dive in
  - Capture lessons learned
    - Constant improvement

Further reading

- *The Security Development Lifecycle*, Howard and Lipner, Microsoft Press
- *Software Security: Building Security In*, McGraw, Addison Wesley
- OWASP
- "Build Security In" portal, http://BuildSecurityIn.us-cert.gov
- Secure Coding Mailing List, http://www.securecoding.org

Kenneth R. van Wyk
KRvW Associates, LLC

Ken@KRvW.com
http://www.KRvW.com


Designing & Implementing Secure Applications
Secure Coding
Principles & Practices
O'REILLY
Mark G. Graff & Kenneth R. van Wyk