Doing the Unstuck

How Rugged Cultures Drive Biz & AppSec Value
Joshua Corman  @joshcorman

- Director of Security Intelligence for Akamai Technologies
  - Former Research Director, Enterprise Security [The 451 Group]
  - Former Principal Security Strategist [IBM ISS]

- Industry:
  - Co-Founder of “Rugged Software” www.ruggedsoftware.org
  - Faculty: The Institute for Applied Network Security (IANS)
  - 2009 NetworkWorld Top 10 Tech People to Know
  - Ponemon Institute Fellow
  - BLOG: www.cognitivedissidents.com

- Things I’ve been researching:
  - DevOps
  - Security Intelligence
  - Chaotic Actors
  - Espionage
  - Security Metrics
A Personal Bit...
Passionate
Purposeful
Principled
Protector
Provider
Honest
Courageous
Consequential
Unreasonable
A Fool
Are We Getting Better...
No
Is it getting better?

Or do you feel the same?
Will it make it easier on you now?
You got someone to blame...
How would you know?
By which criteria?
Constant Change

Evolving Threat
Evolving Compliance
Evolving Technology
Evolving Economics
Evolving Business

Cost Complexity Risk
Why It Matters...
WHAT

WHY

HOW

WHAT

http://www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action.html
Consequences: Value & Replaceability

http://blog.cognitivedissidents.com/2011/10/24/a-replaceability-continuum/
Dependence
Consider...

s/Software/Vulnerability/
Consider...

s/Connected/Exposed/
Consider...

Our challenges are not technical... but cultural
OWASP Top 10

“We can eliminate SQLi in our lifetime”
Activity

Effect
Symptoms

Root Causes
Easy

Important
80/20
Best Practices

aren’t
Good Enough isn’t
Incentives
What you can do about it...
Pick one:

- Make Excuses
- Make Progress
**HDMoore’s Law**

Adversary Classes:
- Espionage: Red
- Organized Crime: Orange
- Chaotic Actors: Yellow
- Casual Attacker: Green
- Auditor/Assessor: Purple

Adversary Centric

- Actor Classes
- Motivations
- Target Assets
- Impacts
- Methods
Rugged DevOps: IT @ Ludicrous Speed!

LUDICROUS SPEED GO !!!
Countermeasures
Situational Awareness
Operational Excellence
Defensible Infrastructure
Countermeasures
Situational Awareness
Operational Excellence
Defensible Infrastructure
Countermeasures

Situational Awareness

Operational Excellence

Defensible Infrastructure
Experimentation

An untested hypothesis is a wish
FAST
Are You Rugged?
HARSH
UNFRIENDLY
THE MANIFESTO
The Rugged Manifesto

I am rugged... and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.
I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.
Rugged?
www.ruggedsoftware.org

https://www.ruggedsoftware.org/documents/

CrossTalk
Rugged-ities

- Availability
- Survivability
- Defensibility
- Security
- Longevity
- Portability

Source: Wendy Nather (at the time, a CISO)
Rugged DevOps Success

- Vertical: Financial
- Business: Money management firm
- Implemented Rugged DevOps to quicken the change cycle and tighten the security
- Results:
  - Increased from quarterly change cycle, to daily changes, 46 average a month.
  - Reduced failed changes from 17% to 4%
  - Reduced IT audit exceptions to zero
Our Commitment to Rugged

CabForward is committed to the highest standards of application and network security for all of our client applications. We secure our infrastructure, ensure our data is protected, build defenses against common threats, practice rugged software development methodologies, and carefully review our code. CabForward has always believed in transparency; in fact, it’s part of the CabForward DNA. We strive to deliver safer, more effective, defensible software and should you or someone you trust choose to validate it; we’re completely open for review.

Infrastructure Control

As we move into a cloud services delivery model, we have made significant investments in best of breed service providers. In our case, we leverage our relationships with both Heroku & Engine Yard to provide the highest level of security and control available. If we were to mimic the hardened infrastructure of either of these providers locally, the costs would be in the hundreds of thousands if not low millions of dollars. We move quickly; we are agile and we leverage the battle-hardened, magic quadrant cloud based service providers.

Application Control

We leverage frameworks that allow us to reduce exposure to the most common exploits. We avoid dangerous software development frameworks that have extreme unresolved or non-defensible vulnerabilities. While we are exploit aware, we choose frameworks that allow us agility in the cloud. Code quality and security is absolutely critical, but the environment it runs on is just as important. We have an active interest in local security scene. We attend the local security conferences and we take to heart rugged security principles in our core product design.

Data Protection

There is no higher priority to us than protecting your data. In order to achieve this goal, we have adopted a ‘rugged’ approach to authentication and access control. This common defense applies across all of our clients and allows us to react quickly to new exploits. Again, we leverage
A declaration of intent & recognition...
The Rugged Summit
We don’t all agree
Dorothy, why do some AppSec guru’s hate Rugged?
PICTURE OF A Campfire "story"
The Rugged Bank Security Story

Commitment: Brick-and-mortar banks protect money with vaults, guards, and alarms. As we move these operations to cyberspace, everyone should expect even better protection of their money and financial information. RuggedBank is committed to the highest standards of application and network security for our RBOnline application. We secure our infrastructure, ensure data is always protected, build defenses against injection and other application attacks, practice rugged software development, and carefully verify our code. At the core of our security is a commitment to transparency – across our protections, processes, and even potential problems.

Infrastructure Control
RBOOnline security depends on maintaining control of our physical and network infrastructure. We are hosted in a secure data center, managed by trusted staff, and our systems are kept hardened, patched, and up-to-date. Our network is defended and segmented by firewalls and we detect and block both network and application attacks.

Application Control
All our data protections depend on having software that is resistant to injection or other attacks that rob us of control of our systems. We have strict rules around data handling and interpreter use to prevent injection. In addition we ensure the application is always available and ready for use.

Data Protection
Protecting your data is our highest priority. Our primary defense is universal authentication and access control. As a secondary defense, we also use strong encryption everywhere data is transmitted or stored. To ensure that these protections are not bypassed, we have established extensive protections against injection and other attacks.

Rugged Development
To make sure that our application is designed and implemented securely, we follow a secure development lifecycle. All our developers are trained in using our standard security defenses. We have performed extensive threat modeling and minimized our attack.

Security Verification
An independent team performs architecture analysis, code review, and penetration testing on our application. We use a custom test suite and automated security tools to double-check for vulnerabilities. We are committed to finding and eliminating

Transparent Security
Without information, good security decisions are impossible, so we are committed to ensuring that you understand the protections that we have provided. We will notify you of any security issues that might affect your business. You can export your data from
Rugged by Role

- Executives CIO/CTO
- Security “Analysts”
- Architects
- Developers
- Testers
- Program Managers
Linkage and Efficiency

CIO  Architect  Developer  QA

[Diagram showing the linkage and efficiency between CIO, Architect, Developer, and QA with some areas highlighted in red.]
To be added from the Rugged Summit

- Buying and selling software
- Understanding the entire software supply chain
- Network security, physical security, database security, etc...
- Other types of software projects, including legacy code, outsourced code, libraries, etc...
- Enterprise level security as opposed to individual projects
Experimentation
An untested hypothesis is a wish
Operational & Attitude
HONEY BADGER
DON'T CARE
Make it better
THANK YOU
My Collaborators
Joshua Corman

[Knowledge Seeker | Zombie Killer]

Twitter: @joshcorman

BLOG: http://blog.cognitivedissidents.com

@RuggedSoftware  @RuggedDevOps

http://RuggedSoftware.org