Network profiling for high assurance survivability

Mike Burmester

Joint work with Owen Redwood

Center for Security and Assurance in IT, Florida State University

MITACS: Network Security and Cryptography

Toronto, Thursday 24th June 2010, 10.00-10.30am

Talkthrough

1. Background
   - *the White House Cyberspace Policy Review*
   - *threat based decision making*
2. Trust Management networks
3. Variable threat level environments
4. Threat based decision making
5. A Markov analyzer
   - *Markov Chains*
   - *anomaly detection*
   - *profiling metrics*
6. Conclusion

Background

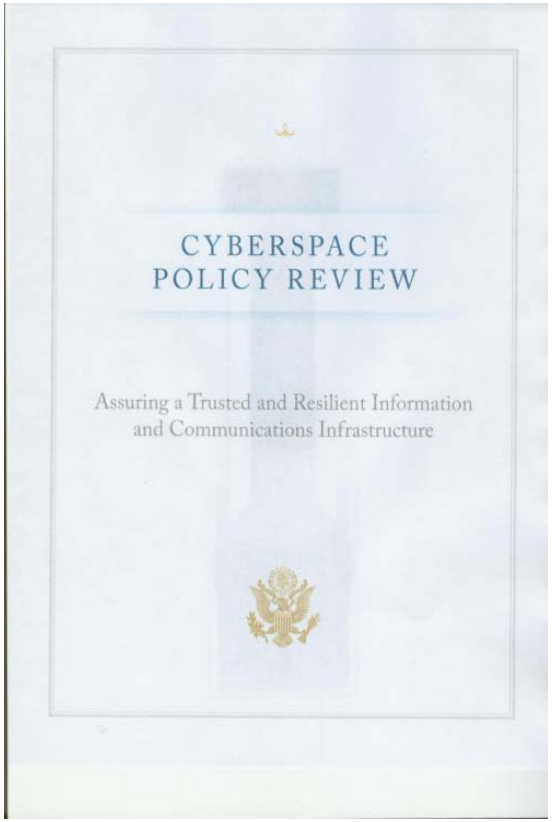
In Feb 2009 the President directed the NSC and the HSC to conduct a blank slate review and assess U.S. policies and structures for the cyberspace

The task of the *Cyberspace Policy Review* was to review plans, programs and activities and develop

- *Policy and Standards*
- *Technologies and Strategy*

for a strategic framework for cybersecurity

The CPR was published in March 2009



"...our approach over the past 15 years has failed to keep pace with the threat."

Near-term plan

- Prepare a national strategy
- Initiate a public awareness and education campaign to promote cybersecurity
- Formulate coherent unified policy guidance for cybersecurity activities that clarifies roles and responsibilities . . .
- Prepare a cybersecurity incident response plan
- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests . . .
- Support education programs and R&D research to ensure the Nation's ability to compete in the information age economy

Mid–term plan

- Expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government
- Develop a framework for R&D strategies that focuses on game-changing technologies . . . to enhance the security, reliability, resilience, and trustworthiness . . .
- Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict . . .
- Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology innovations

Comprehensive National Security Initiative, RSA -03/2010

- Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections
- Deploy an *intrusion detection system* of sensors across the Federal enterprise
- Deploy *intrusion prevention systems* across the Federal enterprise
- Develop a government-wide cyber counter intelligence plan

National Security Initiative

- Expand cyber education
- Define and develop enduring "leap-ahead" technology, strategies, and programs
- Define the Federal role for extending cybersecurity into critical infrastructure domains
- Develop enduring deterrence strategies and programs

Methodology for Security

Resiliency

- Against physical damage, unauthorized manipulation, and electronic assault.
- A risk mitigation strategy with focus on

  devices that access the infrastructure
  the services provided by the infrastructure
  the means of moving storing and processing information
- A strategy for prevention, mitigation and response

Encouraging innovation

- Harness the benefits of innovation
- Not create policy and regulation that inhibits innovation

National Security Initiative
Intrusion Detection

Einstein 2 capability

- *Signature-based sensors* analyze network flow information to identify potential malicious activity : *these detect only copycat type attacks*

Intrusion Prevention

Einstein 3 capability

- *Real-time full packet inspection and threat-based decision-making* on network traffic entering/leaving the Executive Branch networks
- Identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response
- Automatically detect and respond appropriately to cyber threats before harm is done, providing dynamic defense

Einstein 3 capability *will not detect attacks that mimic normal behavior*

Threat based decision making

- Threat-based decision-making on network traffic however may deal with the consequences of unpredictable attacks
- Markovian profiling is a stochastic analyzer that can be used for monitoring traffic/client behavior

Trust Management networks

- Scalable AC management structures (information flow systems)
- A typical model for TM networks are the Bell-LaPadula Access Control systems
  - Users have clearance levels
    - *a user's clearance is based on that user's reputation and trustworthiness*
  - Resources have classification levels
    - *a resource's classification is determined by its the sensitivity*
  - A user that is deemed eligible to a access a resource is granted access
    - *the user's clearance dominates the object's classification*

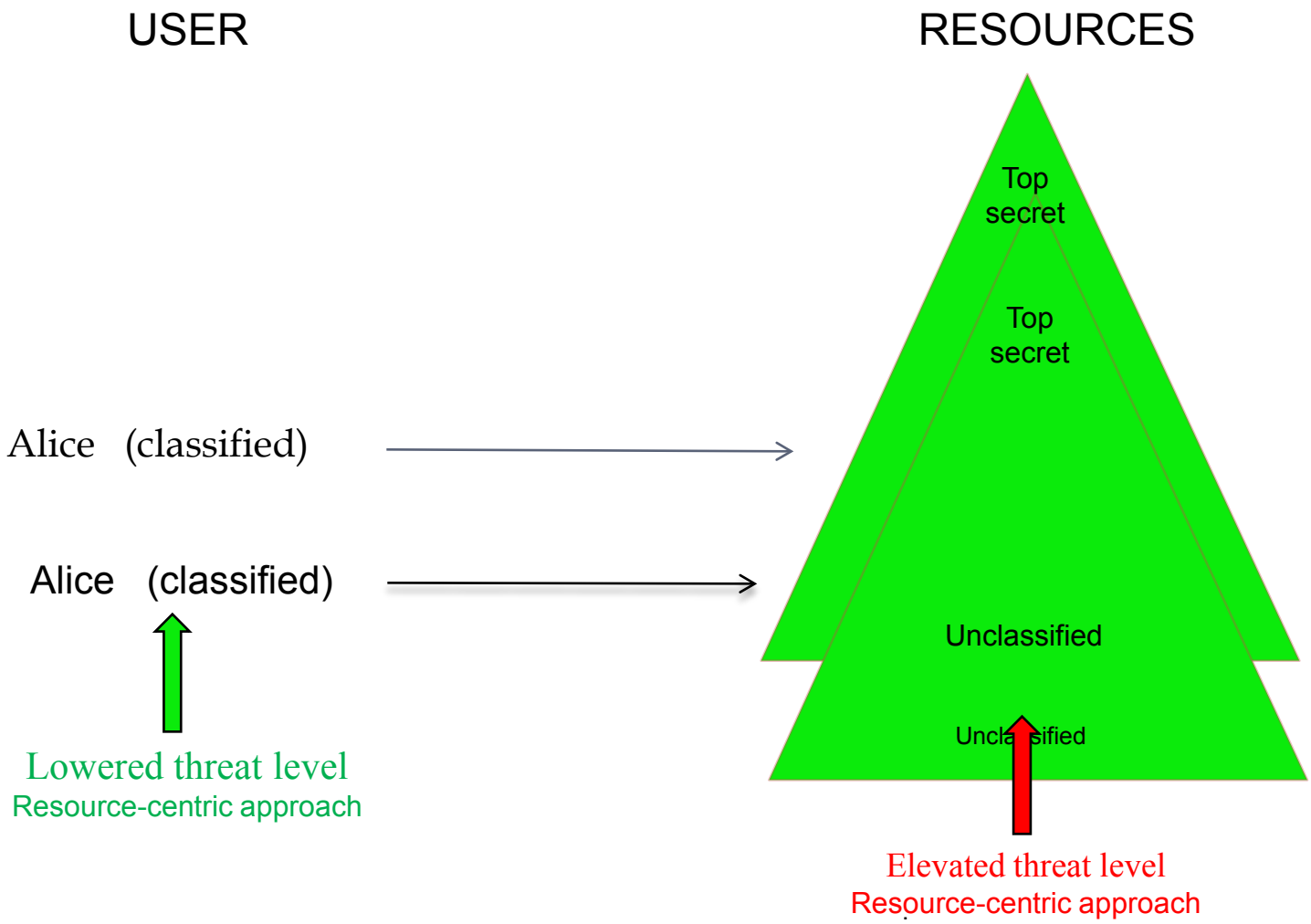
Variable threat level systems

- While the user is in possession of the allocated resource, if the threat level is elevated, access may be *rolled back*
  - *implemented by lowering the user's clearance (client centric)*
  - *implemented by raising the resource classification (resource centric)*
- A resource rollback can preserve, branch-off, or delete changes made to the resource when the access is rolled back

Variable threat level systems

- Threat levels are a high-level construct of the security policy of the network
- As the *threat level* θ increases (decreases), security is tightened (relaxed)
- Tightening (relaxing) security influences access control
  - *domain: the classification level of objects is raized (lowered)*
  - *client: the clearance level of the subject is lowered (raized)*
- The *threat level* layer is above the MAC/ DAC or other AC layers

Variable threat level systems



A Markov Anomaly Analyzer

The problem

- Design a TM system that can automatically rollback access to network resources so as to protect digital assets from malicious attacks in real-time and assure system survivability

A Markov Anomaly Analyzer

Start with a new rollback policy

- Resources are be rolled back when the
  - *domain (network) traffic appears to be anomalous*
  - *client behavior appears to be anomalous*
- In order to detect anomalies, we need a baseline with which to compare events
- We employ a Markov Chain model that builds a normal behavior profile for
  - *the domain and the client*

Markov Chains

- *Markov chains* are a stochastic tool for which the probability of the *next* state in a sequence of events is determined by the previous event state
- *Markov chains of order m* are similar, except that they rely on the past *m* states to predict the probability of a next state
- The Markov probability distribution is defined by a stochastic matrix with each entry being the probability of going from one state to another

Dynamic anomaly detection

- The traditional approach is to use static thresholds to address *anomalous* events
- We propose a dynamic threshold mechanism that is influenced by the
  - *the prevailing threat level in the domain and*
  - *the resources that can be accessed by the client*
- Despite behavior being anomalous, it may still be authorized
- Anomalous behavior is simply *atypical,* not necessarily malicious

Our Basic Assumptions

- Typical user behavior in security-critical TM networks can be profiled dynamically
- There is a cost-metric for describing the security-sensitivity of resources in a network
- The network can be isolated/secured to train the Markov application to develop normal behavior profiles.
- It is not always possible to distinguish between atypical and malicious behavior

The Markov Anomaly Analyzer

- We have a *domain* analyzer and a *client* analyzer, which report anomalies
  - *The domain analyzer can operate on servers or routers*
  - *The client analyzer can operate with root-permission on the client's machine*
- The analyzer monitors both network traffic and client requests: in particular at the
  - *the source and destination*
  - *the service provided to the client*
  - *the permissions needed for the service (if any)*

Other Analyzer Metrics

- The client analyzer uses resource-centric metrics to analyze traffic that include:
  - *suspicious resource access pairing,*
  - *average access time per resources,*
  - *the type of resource, and*
  - *the average access statistics of each type of resource*
- These metrics are primarily designed to defend against:
  - *need-to-know violations*
  - *resource-crawler attacks*

What the Analyzer Reports

When an anomaly is detected

- The events that triggered it (packet stream)
- The probability distribution of that series of events
- The confidence with which the analyzer predicts that they are anomalous

When no anomaly is detected, it simply reports that the traffic is normal

How the TM Agent works

- The TM Agent is responsible for changing the threat level in the TLR layer
- We do this by having two counters: one for the domain, the other for the client
- The counters are initialized at 0 and bounded by the highest/lowest threat levels tl_{lower} / tl_{raise}

  ---*these can be parameterized*
- The threat level is lowered/raised when these thresholds are crossed
- The counters are raized when traffic is anomalous, and lowered otherwise.

How the TM Agent works

- *Behavior profiling*

  Monitor behavior (of domain/ client) over a period of time to get the a distribution μ
- The distribution μ is continuously updated
- The states s of the system are partitioned into S_{normal} and $S_{anomalous}$

  ---this can be parameterized
- *Markov μ-prediction*

  s_{next} = next state of the system, c_{dom} = a system parameter

  Prob[*traffic behavior is anomalous* | $s_{next} \in S_{anomalous}$] = c_{dom}

  Prob[*traffic behavior is normal* | $s_{next} \in S_{normal}$] = 1

The Markov TM Agent

- The Markov agent works by modifying the permissions (of clients and/or domains) to address anomalous behavior
- At any given time, for any given client we have the following four cases to consider:

Cases	μ_{domain}	μ_{client}	Notes
1	1	1	*All traffic is normal*
2	1	c_{domain}	*Domain traffic is anomalous*
3	c_{client}	1	*Client traffic is anomalous*
4	c_{client}	c_{domain}	*Domain & client traffic is anomalous*

Conclusion

- We have proposed a framework for a *dynamic, real-time,* system defense
- This framework allows us to restrict adversarial attacks to those that appear normal to the TM analyzer
- Attacks that cause the behavior of the domain or client to deviate from normal are thwarted

Thanks for listening!

Bibliography

O. Redwood and M. Burmester. *Markov anomaly modeling for Trust Management in variable threat environments*. In Proc. IEEE SE, 2010.

M. Burmester, P. Das, M. Edwards, and A. Yasinsac, *Multi-domain Trust Management in variable threat environments using rollback-access*. In Proc. Military Communications Conference (MILCOM 2008). IEEE, 2008.

M. Burmester, P. Das, M. Edwards, and A. Yasinsac. *Multi-domain Trust Management in variable threat environments – a user-centric model*. In Proc. Military Communications Conference (MILCOM 2009). IEEE, 2009