A Deterministic Profiling Approach to support Behaviour Anomaly Detection

Rukmal Fernando and
Vidura Gamini Abhaya

Informatics Institute of Technology

The line-up…

- Quick look at the Problem area
- The Hypothesis and high-level solution
- The architecture
- The Prototype
- The achievement
- The future outlook
- Q&A…

The fundamental problem

- How secure are passwords?
  - Human weakness, discovery, guessing, brute-force, human engineering, attacks, sniffing
- Authentication protocols have own weaknesses
- Biometrics – Not accurate, can be impersonated
- Intrusion Detection focused on detecting attacks
- All factors lead to high impersonation risk
- The key problem: How can an impersonation be detected?
  - System “assumes” that authentication was successful and accurate

Hypothesising a solution…

- A valid user has specific long-term objectives. This would result in recognizable patterns in user's behaviour
- An impersonator with malicious intent has objectives clearly different from a valid user. This should manifest itself in a change of behaviour.
- How do we detect this change?

Behaviour Anomaly Detection

- The process of creating a profile of typical behaviour, and identifying deviations
- A field of active research
- Uses a number of inputs…
  - System calls, command sequences, system audit data (e.g. CPU usage)
- … and a number of techniques
  - Artificial Neural Networks, Support Vector Machines, Bayesian Networks, Statistical anomaly detection, Data mining etc.

Problem solved?

- Artificial Intelligence
  - Problems with predictability and controllability
- Statistical approaches
  - Require large history logs
- Our approach
  - Compact, yet descriptive profile
  - Privacy preservation
  - Predictable, deterministic and controllable

The high-level solution

- Monitor Network Traffic to obtain behaviour information
  - Achieved via ‘packet capture’
  - Permits heterogeneous, real-time operation
- Create a ‘Profile’ of the User and look for anomalies in behaviour
- User Monitoring at the host by an ‘Agent’, controlled by central server with monitoring capabilities
- Use a Rule-base to evaluate each user action and assign a score based on past behaviour

The Profiling Process

Scoring

If ($A_A > A_I$)

Score = { (A_A / A * $Score_{old}$ * Count) + $Score_{new}$}
* (Count + 1) / Count

Else

Score = {((1 - A_I / A) * $Score_{old}$ * Count) + $Score_{new}$}
* (Count + 1) / Count

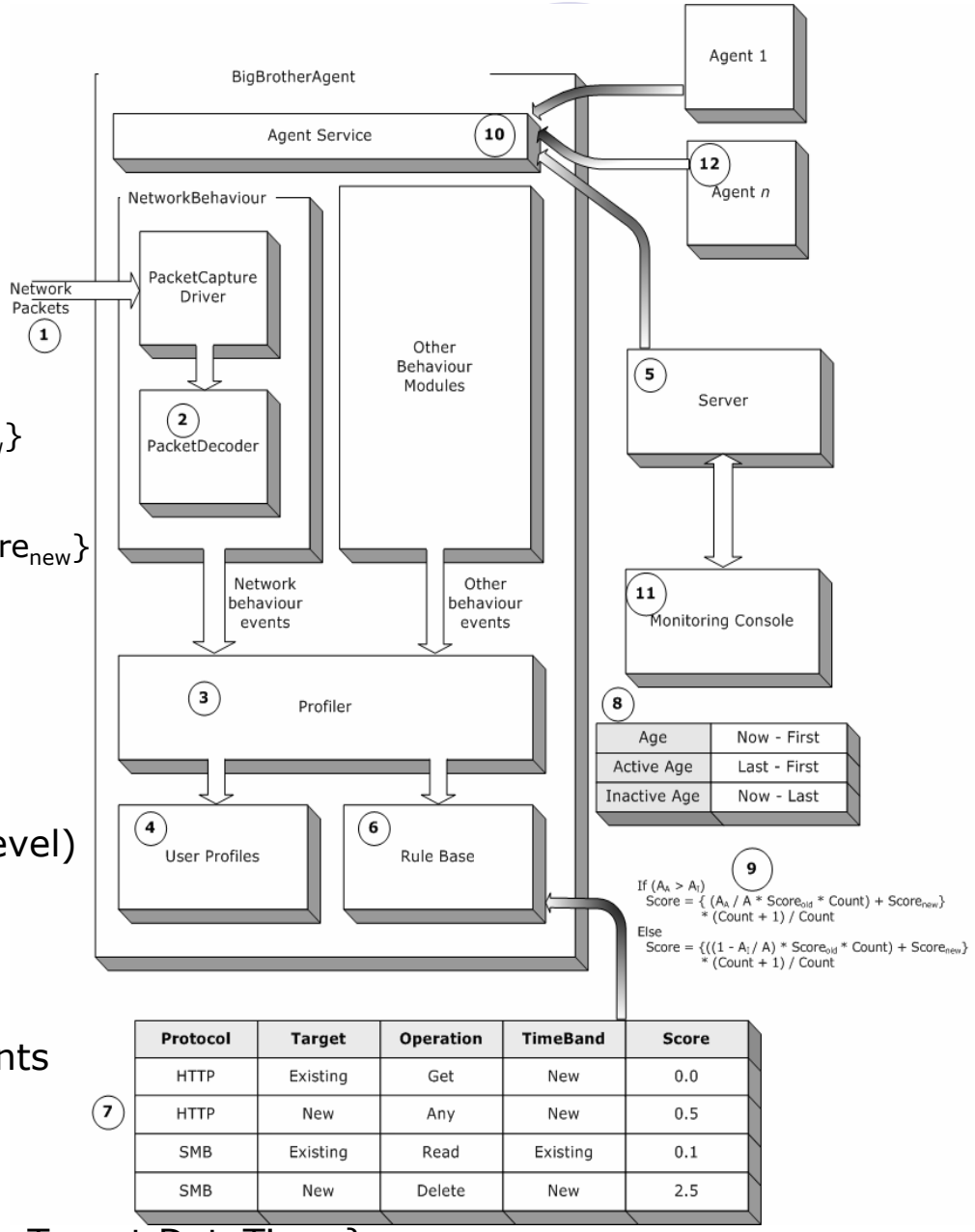
Impersonation risk assessment:

Primary alert: (event score ≥ AlertLevel)

Secondary alert: (Profile score ≥ ThreatLevel)

Mode:

IsMonitoring = ∑Count ≥ MinLearningEvents



3

Profile Event = { User, Protocol, Operation, Target,DateTime }

Equation 1

Profile Structure

```
<Profile username="stu01067" FirstEvent="4/25/2005 8:15:18 PM" LastEvent="4/25/2005 8:15:20
PM" EventCount="161" >
  <protocol protocolname="smb">
    <target id="192.168.25.6">
      <operation operationName="Open" >
        <Entry Index="1" First="63260646855819505 6" Last="632607596135338896" Count="103" Score="0.08252293" Status="1" />
        <Entry Index="4" First="632606468558195056" Last="632607596135338896" Count="103" Score="0.08252293" Status="1" />
        <Entry Index="10" First="632606468558195056" Last="632606829477070912" Count="41" Score="0" Status="0" />
        <Entry Index="11" First="632607332481623472" Last="632607596135338896" Count="62" Score="0.09480664" Status="1" />
        <Entry Index="24" First="632606468558195056" Last="632607596135338896" Count="103" Score="0.0822293" Status="1" />
      </operation></target>
  </protocol>
  ……
</Profile>
```

```
<Entry Index="4" First="6326064685581950 56"
     Last="
     Score=
```

```
<!-- ?xml version="1.0" standalone="yes" name="SMB Command list" -->
<Commands>
  <command number="0"   type="Create"  commandName="Create Directory" />
  <command number="1"   type="Delete"  commandName="Delete Directory" />
  <command number="2"   type="Open"    commandName="Open File"/>
  <command number="3"   type="Create"  commandName="Create File" />
  <command number="4"   type="Close"   commandName="Close File" />
  <command number="5"   type="Close"   commandName="Flush File" />
  <command number="6"   type="Delete"  commandName="Delete File" />
  ……
</Commands>
```

Rule base and Scoring

Protocol	Target	Operation	Score
HTTP	Existing	Get	0.0
HTTP	New	Any	0.5
SMB	Existing	Read	0.1
SMB	New	Delete	2.5

If ($A_A > A_I$)

$$Score = \{ (A_A / A * Score_{old} * Count) + Score_{new}\} * (Count + 1) / Count$$

Else

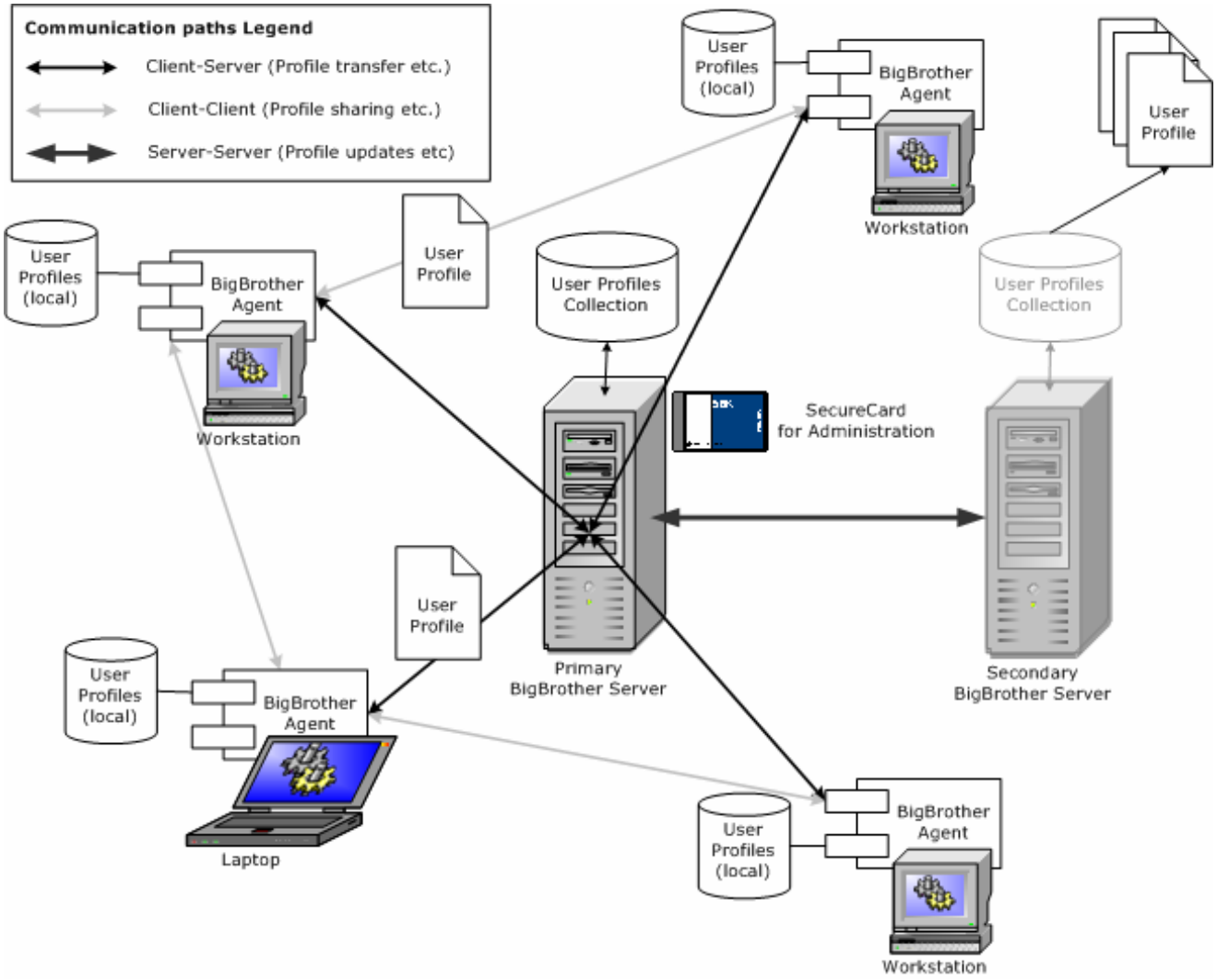
$$Score = \{((1 - A_I / A) * Score_{old} * Count) + Score_{new}\} * (Count + 1) / Count$$

Where A = Age, A_A = Active age and A_I = Inactive age

Deploying the Prototype

- The Agent
  - Deployed on each host to be monitored as a Windows Service
- The Server
  - Deployed to a few select hosts as a Windows Service
  - Must be secured – Key pair, Rules, Profiles etc.
- The Monitoring console
  - Windows application to be run on demand

The Architecture



Features of prototype

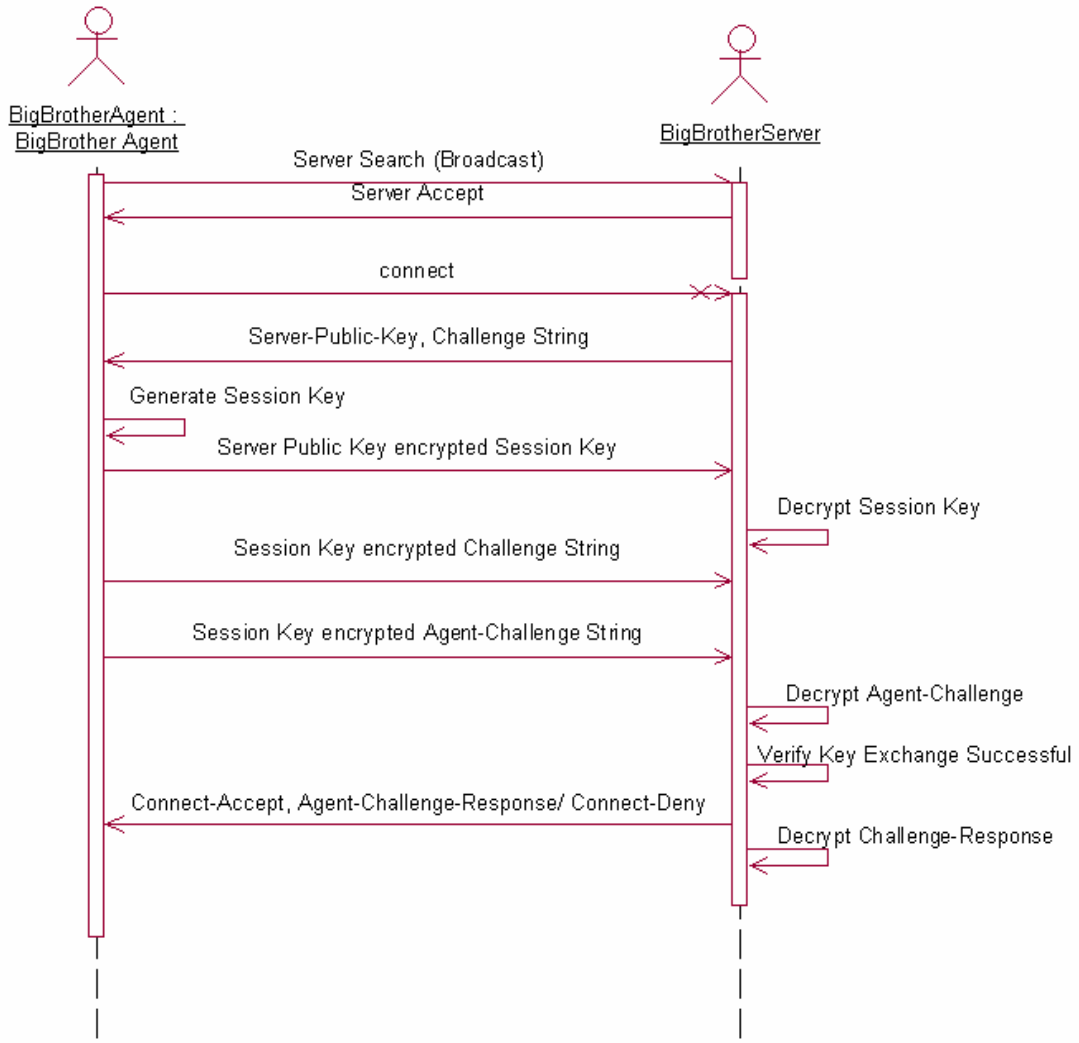
- Parameter based profiling
- Rule set allows different activity types to have varying threat levels
- XML-based, lightweight, secure protocol
- No need for activity logs, and profile size is more-or-less constant after learning period
- Preserve privacy by encrypting target information etc. with public key
- Dynamic discovery, recovery of servers
- Agent can operate either on-line or off-line
- Open, extensible, secure framework
- Controllable and predictable due to Rule and Scoring approach
- Handle “Concept Drift”

Securing the solution

- Mutual Authentication phase
  - Short-term Session Key exchange
- Encryption of messages, stored rule-sets and profiles
- Use of Data Protection API for storing sensitive information
- Secondary Authentication mechanism for ultimate control
- Windows authentication for monitoring
- Use of dedicated credentials for services

Mutual Authentication phase

- Use RSA asymmetric encryption to securely exchange an AES session key
- Session key and Server public key cached for future checking



Deterministic profiling

- Rule-base can be configured on-line in real-time
- Scoring algorithm used to "Age" existing score and average it with new score
- In *Learning* state build profile, in *Monitoring* state evaluate and update
  - $IsMonitoring = \sum Count \geq MinLearningEvents$
  - See equation 4
- Take actions on
  - Single event's score exceeding threshold
  - Profile's threat level exceeding threshold

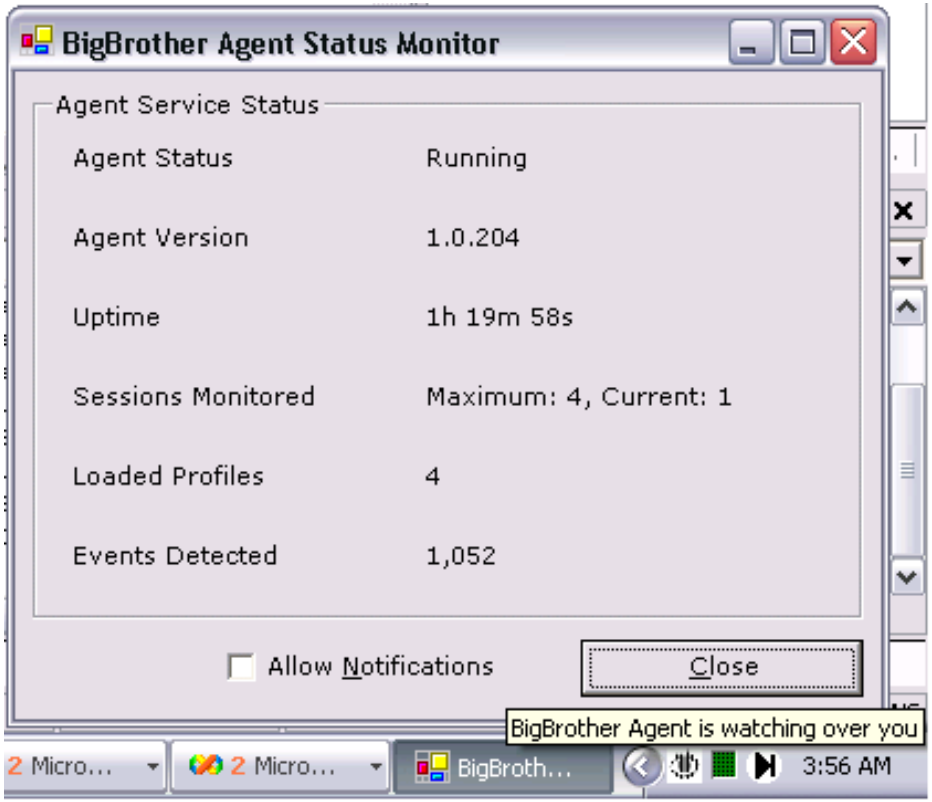
Privacy concerns

- Sri Lanka, UK, USA etc. offer no legal right to resist monitoring
  - "Control Test" in Sri Lanka may apply
- Use of PKI to prevent profile decode
- Fully automated process limits disclosure

The achievement

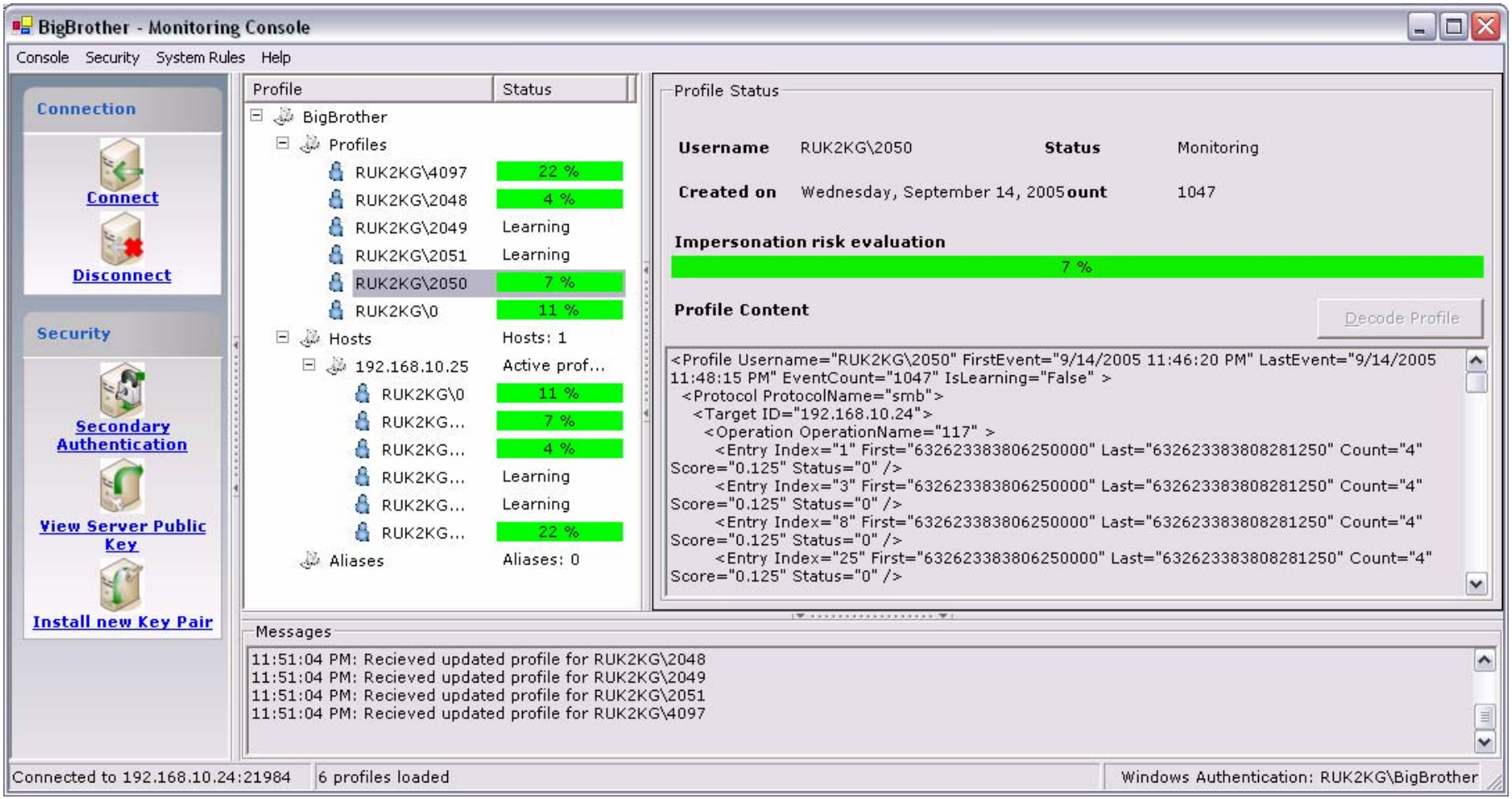
- A functional prototype that was very promising
  - In confirming the hypothesis behind behaviour anomaly detection
  - In demonstrating a deterministic profiling approach
- Resulted in a paper presentation at the IEE Young Members' Sessions, 2005
- Prototype judged by panel from BCS and received Silver award at National Best Quality Software Awards, 2005 (tertiary category)

Observing the Agent…



Informing the user that he his actions are being monitored –
*"BigBrother Agent is **watching over you**"*

The Monitoring console



Profiles shown decoded after secondary authentication

Key technologies

- Visual C++ ATL/ COM
- Visual C#.Net and .Net class libraries
- WinPcap for capturing packets
- UDP as transport mechanism for protocol
- Encryption with Advanced Encryption Standard - AES (Rijndael)
- XML based profiles, rule base, protocol messages, configuration etc.
- Windows Data Protection API for storing long term keys, session keys etc. securely
- BZip2 library for compressing profiles etc.
- Status logging with the Windows Event Log
- Modelling and documentation with UML

The road ahead…

- While promising, testing was not adequate to clearly achieve target
- Needs a lot of time-input to fine-tune the various parameters
- But nevertheless seen as a positive contribution to the world of knowledge and a stepping stone for future work

Summary

- Behaviour Anomaly detection as means of detecting Impersonations is an active research area
- Our project introduces a new approach to try and make this process deterministic, secure and privacy-preserving
- Results are promising, and a foundation for future work
- A quick “Thank you” to all who supported it…
- And to you for your attention at this moment!

Q & A