NTT Confidential
Disclosed to Hybrid Application Security Ltd.

Innovative R&D by NTT

Our test scenario

NTT Secure Platform Laboratories

Copyright©2014 NTT corp. All Rights Reserved.

Agenda

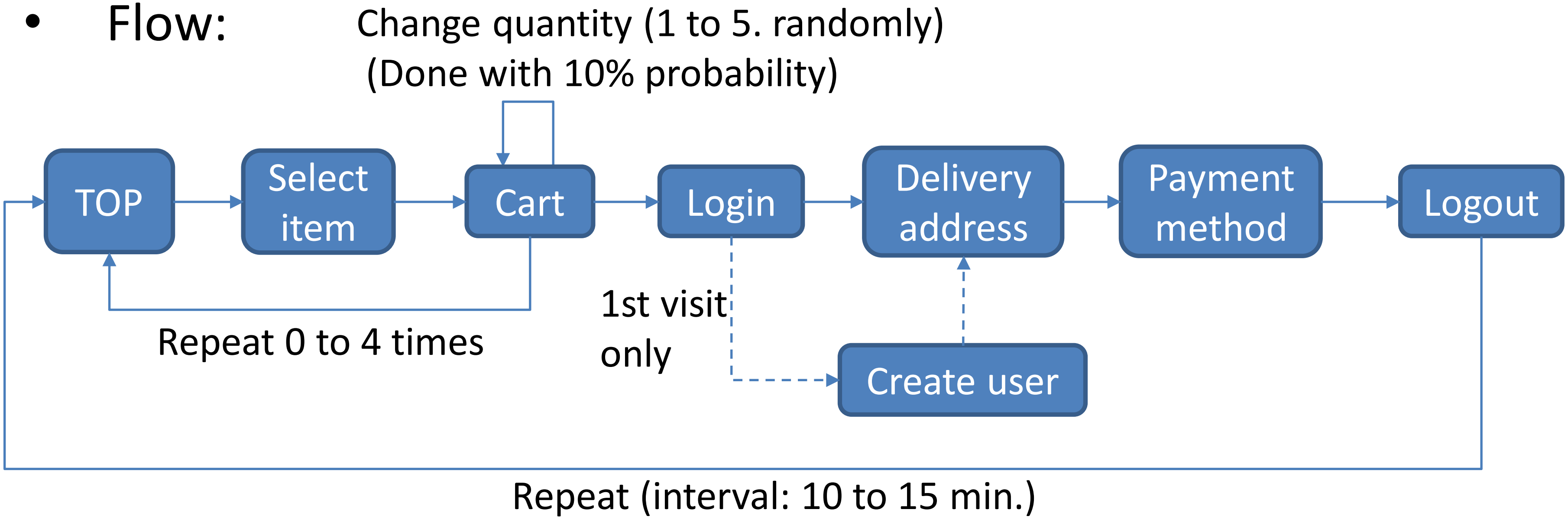
- Learning scenario
- Attack scenario and prospective alerts
    1. Leaked password list attack
    2. Known password attack, e.g. phishing or social engineering
    3. Session hijacking
    4. Man In The Browser (MITB)
    5. Mass user registration by script

Copyright©2014 NTT corp. All Rights Reserved.

Learning scenario

We cannot use real traffic for Lab test. We generate pseudo traffic in the following manner.

- Target: EC sites (*Spree commerce* demo site)
- User: 13 users (Half of them use static IP address, the rest use dynamic IP address. All IPs belong to Japan.)
- Flow:



Copyright©2014 NTT corp. All Rights Reserved.

Learning scenario (contd.)

- Purchasing items are selected randomly.
- Delivery address is fixed for each user.
- 1/3 of users pay by credit card every time, 1/3 of users pay by check every time, and the rest users select payment method randomly for each access.
- Page transition interval is 2 to 4 sec. for pages without text input form, 9 to 11 sec. for pages with text input form.
- A few users login before selecting items.
- User-agent header is Firefox’s one.

We plan to make learning traffic in this way for 3 to 5 days by script or JMeter.
We’d like to evaluate weather Telepath can learn properly and make effective rules with this traffic.

Copyright©2014 NTT corp. All Rights Reserved.

1. Leaked password list attack

- Overview
  - Attacker attempts to login repeatedly with ID and password on the list which is leaked from other sites.
- Flow and prospective alerts

No.	Action	Prospective alerts	Telepath's Algorithm
1	Access to login page directly	Abnormal access. Normal users tend to visit TOP page first.	Navigation
2	Post ID and password	They are posted instantly by a script. It takes 9 to 11 sec. for normal users.	Click speed
		Normal user's passwords are 6-8 length but some passwords on the list are 10 or more length.	Parameter length
3	Repeat #1 and #2 by a script	Anomaly access. Normal users tend to continue purchasing items after the login.	Navigation

Copyright©2014 NTT corp. All Rights Reserved.

2. Known password attack

- Overview
  - Attacker knows legitimate ID/password pair and logins with them. This happens in the case of Phishing and social engineering.
- Flow and prospective alerts

No.	Action	Prospective alerts	Telepath's Algorithm
1	Access to login page from TOP page using China's IP address and IE as client.	Abnormal access. Normal users tend to select items before login.	Navigation
2	After the login, select items.	Access from China. Normal users access from Japan.	Geography
		Browser is IE. Normal users use Firefox.	URL Analysis (Header)
3	Go to cart and set quantity to 100	Parameter anomaly. Normal users purchases 1 to 5 quantities.	Numeric analysis
4	Enter a delivery address	Parameter anomaly. The address is different from usual one.	Menu choices Text analysis

Copyright©2014 NTT corp. All Rights Reserved.

3. Session hijacking

- Overview
  - Attacker steals session ID and hijacks user's session.
- Flow and prospective alerts

No.	Action	Prospective alerts	Telepath's Algorithm
1	(User) Access to TOP page, select items and login		
2	Access from other client with same session ID, using China's IP	Src IP changes suddenly.	Velocity
		Access from China. Normal users access from Japan.	Geography
3	Select items, go cart and set quantity to 100	Parameter anomaly. Normal users purchases 1 to 5 quantities.	Numeric analysis
4	Enter a delivery address	Parameter anomaly. The address is different from usual one.	Menu choices Text analysis

Copyright©2014 NTT corp. All Rights Reserved.

4. Man In The Browser (MITB)

- Overview
  - Attacker gets control of browsers and alters parameters.
- Flow and prospective alerts

No.	Action	Prospective alerts	Telepath's Algorithm
1	(User) Access TOP page, select items and login		
2	Access from the same client.	(This may not be distinguished from normal access.)	
3	Select items, go cart and set quantity to 100	Parameter anomaly. Normal users purchases 1 to 5 quantities.	Numeric analysis
4	Alter parameters, insert or delete parameters	Parameter anomaly.	Parameter absence/presence

Copyright©2014 NTT corp. All Rights Reserved.

5. Mass user registration by script

- Overview
  - Attacker tries to register vast amount of users for malicious activities.
- Flow and prospective alerts

No.	Action	Prospective alerts	Telepath's Algorithm
1	Set variable X=0		
2	Access to user registration page and make a user ID=dummyX@example.com	Abnormal access. Normal users tend to visit TOP page first.	Navigation
3	Increment X and repeat #2	Continuous access with similar parameters.	Parameter similarity
		ID/PW are posted instantly by a script. It takes 9 to 11 sec. for normal users.	Click speed

Copyright©2014 NTT corp. All Rights Reserved.