A New Approach to E-Banking

Matthew Johnson matthew.johnson@cl.cam.ac.uk
Simon Moore simon.moore@cl.cam.ac.uk

University of Cambridge, Computer Laboratory

The 12th Nordic Workshop on Secure IT-systems

Outline

Outline

Phishing Attacks

Current Attacks

- Common attacks very simple
  - Just harvest credentials
  - Easy to defend against
  - Aim of current defences
- Complex attacks are easy
  - Real-time attacks—seen in the wild
  - Re-writing trojans—seen in the wild
  - DNS pharming—seen in the wild

Conclusion

Stopping simple attacks will just cause attackers to use complex attacks.

Phishing Attacks

Current Attacks

- Common attacks very simple
  - Just harvest credentials
  - Easy to defend against
  - Aim of current defences
- Complex attacks are easy
  - Real-time attacks—seen in the wild
  - Re-writing trojans—seen in the wild
  - DNS pharming—seen in the wild

Conclusion

Stopping simple attacks will just cause attackers to use complex attacks.

Phishing Attacks

Current Attacks

- Common attacks very simple
  - Just harvest credentials
  - Easy to defend against
  - Aim of current defences
- Complex attacks are easy
  - Real-time attacks—seen in the wild
  - Re-writing trojans—seen in the wild
  - DNS pharming—seen in the wild

Conclusion

Stopping simple attacks will just cause attackers to use complex attacks.

Phishing Attacks

Current Attacks

- Common attacks very simple
  - Just harvest credentials
  - Easy to defend against
  - Aim of current defences
- Complex attacks are easy
  - Real-time attacks—seen in the wild
  - Re-writing trojans—seen in the wild
  - DNS pharming—seen in the wild

Conclusion

Stopping simple attacks will just cause attackers to use complex attacks.

Outline

Secure UI

Secure UI

The key to securing internet banking is transparency for the user in what they are authorizing.

This requires a secure interface to the user, not just to the user's computer.

Secure UI

Secure UI

The key to securing internet banking is transparency for the user in what they are authorizing.

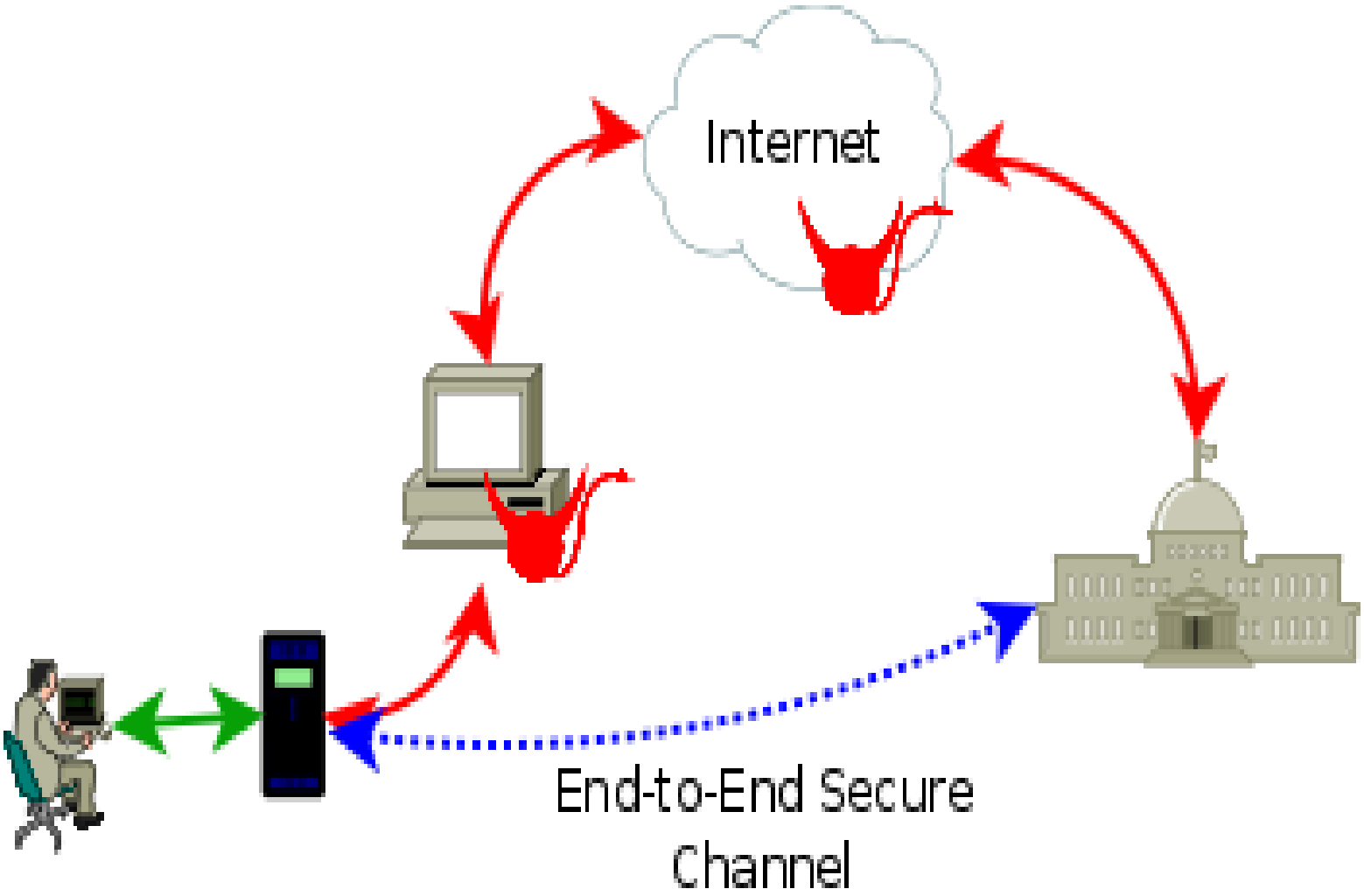
This requires a secure interface to the user, not just to the user's computer.

Outline

Banking Dongle

- Cheap (enough)
- Secure communication
- Display
- Input
- PC can be compromized

Banking Dongle Architecture



Bank–Device Protocol

Protocol

Bank	Device	User
Session Keys →		
	← Key ACK	
Transaction →		
	Transaction →	
		← Auth
	← Auth	

Key

- Encryption with long-term keys
- Session encryption
- Trusted UI

Full Protocol

Bank–Device Protocol

Protocol

Bank	Device	User
Session Keys $\rightarrow$		
	$\leftarrow$ Key ACK	
Transaction $\rightarrow$		
	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth	

Key

- Encryption with long-term keys
- Session encryption
- Trusted UI

Full Protocol

Bank–Device Protocol

Protocol

Bank	Device	User
Session Keys $\rightarrow$		
	$\leftarrow$ Key ACK	
Transaction $\rightarrow$		
	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth	

Key

- Encryption with long-term keys
- Session encryption
- Trusted UI

Full Protocol

Bank–Device Protocol

Protocol

Bank	Device	User
Session Keys $\rightarrow$		
	$\leftarrow$ Key ACK	
Transaction $\rightarrow$		
	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth	

Key

- Encryption with long-term keys
- Session encryption
- Trusted UI

Full Protocol

Bank–Device Protocol

Protocol

Bank	Device	User
Session Keys $\rightarrow$		
	$\leftarrow$ Key ACK	
Transaction $\rightarrow$		
	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth	

Key

- Encryption with long-term keys
- Session encryption
- Trusted UI

Full Protocol

Bank–Device Protocol

Protocol

Bank	Device	User
Session Keys $\rightarrow$		
	$\leftarrow$ Key ACK	
Transaction $\rightarrow$		
	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth	

Key

- Encryption with long-term keys
- Session encryption
- Trusted UI

Full Protocol

Bank–Device Protocol

Protocol

Bank	Device	User
Session Keys $\rightarrow$		
	$\leftarrow$ Key ACK	
Transaction $\rightarrow$		
	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth	

Key

- Encryption with long-term keys
- Session encryption
- Trusted UI

Full Protocol

Outline

Consumer Protection

- Credit cards look out for the bank's interests
- Tills look out for the shop's interests
- Nothing looks out for the customer's interests

Can our device look out for the customer's interests?

Consumer Protection

- Credit cards look out for the bank's interests
- Tills look out for the shop's interests
- Nothing looks out for the customer's interests

Can our device look out for the customer's interests?

Consumer Protection

- Banks dispute claims of phantom transactions. . .
- . . . yet claim they can't disclose keys
- Customer gets receipts with MACs for valid transactions. . .
- . . . but cannot prove they *didn't* make a transaction

Provide the consumer with a verifiable audit trail which denies phantom transactions.

Consumer Protection

- Banks dispute claims of phantom transactions. . .
- . . . yet claim they can't disclose keys
- Customer gets receipts with MACs for valid transactions. . .
- . . . but cannot prove they *didn't* make a transaction

Provide the consumer with a verifiable audit trail which denies phantom transactions.

Bank–Device Audit Protocol

Protocol

Bank	Device	User
Session Keys		
$\rightarrow$	$\leftarrow$ Key ACK	
Transaction $\rightarrow$	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth, h(previous log entry),h(next log nonce), MAC_D(Transaction)	
$MAC_B(\ldots)$	LOG: Transaction, $MAC_B(\ldots)$, h(previous log	
$\rightarrow$	entry),h(next log nonce), log nonce	

Full Audit Protocol

Bank–Device Audit Protocol

Protocol

Bank	Device	User
Session Keys		
$\rightarrow$	$\leftarrow$ Key ACK	
Transaction $\rightarrow$	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth, h(previous log entry),h(next log nonce), MAC_D(Transaction)	
$MAC_B(\ldots)$ $\rightarrow$	LOG: Transaction, $MAC_B(\ldots)$, h(previous log entry),h(next log nonce), log nonce	

Full Audit Protocol

Bank–Device Audit Protocol

Protocol

Bank	Device	User
Session Keys		
$\rightarrow$	$\leftarrow$ Key ACK	
Transaction $\rightarrow$	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth, h(previous log entry),h(next log nonce), MAC_D(Transaction)	
$MAC_B(\dots)$	LOG: Transaction, $MAC_B(\dots)$, h(previous log entry),h(next log nonce), log nonce	
$\rightarrow$		

Full Audit Protocol

Bank–Device Audit Protocol

Protocol

Bank	Device	User
Session Keys		
$\rightarrow$	$\leftarrow$ Key ACK	
Transaction $\rightarrow$	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth, h(previous log entry),h(next log nonce), MAC_D(Transaction)	
$MAC_B(\dots)$	LOG: Transaction, $MAC_B(\dots)$, h(previous log entry),h(next log nonce), log nonce	
$\rightarrow$		

Full Audit Protocol

Bank–Device Audit Protocol

Protocol

Bank	Device	User
Session Keys		
$\rightarrow$	$\leftarrow$ Key ACK	
Transaction $\rightarrow$	Transaction $\rightarrow$	
		$\leftarrow$ Auth
	$\leftarrow$ Auth, h(previous log entry),h(next log nonce), MAC_D(Transaction)	
$MAC_B(\dots)$ $\rightarrow$	LOG: Transaction, $MAC_B(\dots)$, h(previous log entry),h(next log nonce), log nonce	

Full Audit Protocol

Outline

Software Defences

- Mostly concentrate on common, simple attacks
- Heuristics and blacklists—can't catch all attacks
- Don't stop current attacks
- By definition can't stop a compromised terminal

Token Defences

Tokens

- APACS: must have dual-factor
- Often only window dressing
- Stop simple attacks
- Rarely more

Source

Mobile Phones

- Don't prevent all attacks
- Do we trust mobile phones?

Outline

Internet Shopping

- eBanking is not the only place you perform financial transactions
- Secure internet shopping is desirable
- Verified-by-Visa and SecureCode

Internet Shopping

- eBanking is not the only place you perform financial transactions
- Secure internet shopping is desirable
- Verified-by-Visa and SecureCode

Outline

Conclusion

- Current anti-phishing concentrates on current phishing
- Complicated phishing is easy

- The banking dongle addresses all phishing attacks
- Also provides protection for the consumer

Conclusion

- Current anti-phishing concentrates on current phishing
- Complicated phishing is easy

- The banking dongle addresses all phishing attacks
- Also provides protection for the consumer

Any Questions?

Protocol

$$
\begin{aligned}
M_1 = &\quad I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2} \\
B \rightarrow D: &\quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) && (1) \\
M_2 = &\quad I+1, \text{“}ACK\text{”}, Len, D \\
D \rightarrow B: &\quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) && (2) \\
M_3 = &\quad N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type \\
B \rightarrow D: &\quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) && (3) \\
D \rightarrow U: &\quad \text{transaction} && (4) \\
U \rightarrow D: &\quad Auth && (5) \\
M_6 = &\quad N+1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth \\
D \rightarrow B: &\quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) && (6)
\end{aligned}
$$

Protocol

$$M_1 = \quad I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2}$$

$$B \rightarrow D: \quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) \tag{1}$$

$$M_2 = \quad I + 1, \text{“}ACK\text{”}, Len, D$$

$$D \rightarrow B: \quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) \tag{2}$$

$$M_3 = \quad N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type$$

$$B \rightarrow D: \quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) \tag{3}$$

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = \quad N + 1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

Protocol

$$M_1 = \quad I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2}$$

$$B \rightarrow D: \quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) \tag{1}$$

$$M_2 = \quad I + 1, \text{“}ACK\text{”}, Len, D$$

$$D \rightarrow B: \quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) \tag{2}$$

$$M_3 = \quad N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type$$

$$B \rightarrow D: \quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) \tag{3}$$

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = \quad N + 1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

Protocol

$$M_1 = I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2}$$

$$B \rightarrow D: \quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) \tag{1}$$

$$M_2 = I + 1, \text{“}ACK\text{”}, Len, D$$

$$D \rightarrow B: \quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) \tag{2}$$

$$M_3 = N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type$$

$$B \rightarrow D: \quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) \tag{3}$$

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = N + 1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

Protocol

$$M_1 = \quad I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2}$$

$$B \rightarrow D: \quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) \tag{1}$$

$$M_2 = \quad I+1, \text{“}ACK\text{”}, Len, D$$

$$D \rightarrow B: \quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) \tag{2}$$

$$M_3 = \quad N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type$$

$$B \rightarrow D: \quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) \tag{3}$$

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = \quad N+1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

Protocol

$$M_1 = I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2}$$

$$B \rightarrow D: \quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) \tag{1}$$

$$M_2 = I + 1, \text{“}ACK\text{”}, Len, D$$

$$D \rightarrow B: \quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) \tag{2}$$

$$M_3 = N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type$$

$$B \rightarrow D: \quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) \tag{3}$$

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = N + 1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

Protocol

$$M_1 = \quad I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2}$$

$$B \rightarrow D: \quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) \tag{1}$$

$$M_2 = \quad I + 1, \text{“}ACK\text{”}, Len, D$$

$$D \rightarrow B: \quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) \tag{2}$$

$$M_3 = \quad N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type$$

$$B \rightarrow D: \quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) \tag{3}$$

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = \quad N + 1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

Protocol

$$
\begin{aligned}
M_1 = &\quad I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2} \\
B \rightarrow D: &\quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) && (1) \\
M_2 = &\quad I+1, \text{“}ACK\text{”}, Len, D \\
D \rightarrow B: &\quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) && (2) \\
M_3 = &\quad N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type \\
B \rightarrow D: &\quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) && (3) \\
D \rightarrow U: &\quad \text{transaction} && (4) \\
U \rightarrow D: &\quad Auth && (5) \\
M_6 = &\quad N+1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth \\
D \rightarrow B: &\quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) && (6)
\end{aligned}
$$

Audit Protocol

$$
\begin{aligned}
M_1 = &\quad I, \text{“}INIT\text{”}, Len, D, K_{BD1}, K_{BD2} \\
B \rightarrow D: &\quad \text{“}INIT\text{”}, Len, IV, \{M_1\}_{E_{K_{LT}}}, MAC_{K_{LTM}}(M_1) && (1) \\
M_2 = &\quad I+1, \text{“}ACK\text{”}, Len, D \\
D \rightarrow B: &\quad \text{“}ACK\text{”}, Len, IV, \{M_2\}_{E_{K_{BD1}}}, MAC_{K_{BD_2}}(M_2) && (2) \\
M_3 = &\quad N, \text{“}TRANS\text{”}, Len, D, \text{transaction}, Type \\
B \rightarrow D: &\quad \text{“}TRANS\text{”}, Len, IV, \{M_3\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_3) && (3) \\
D \rightarrow U: &\quad \text{transaction} && (4) \\
U \rightarrow D: &\quad Auth && (5) \\
M_6 = &\quad N+1, \text{“}AUTH\text{”}, Len, D, \text{transaction}, Type, Auth \\
D \rightarrow B: &\quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) && (6)
\end{aligned}
$$

Audit Protocol

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = \quad N+1, \text{“}AUTH\text{”}, Len, D, h(O_{I+1}), h(L_{I-1}), \text{transaction}, Type, Auth, MAC_{K_D}(\text{transaction})$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

$$M_7 = \quad MAC_{K_B}(N, I, \text{“}TACK\text{”}, Len, D, \text{transaction}, h(O_{I+1}), h(L_{I-1}), Type, Auth, MAC_{K_D}(\text{transaction}))$$

$$B \rightarrow D: \quad \text{“}TACK\text{”}, Len, IV, \{M_7\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_7) \tag{7}$$

$$L_I = \quad N, I, Len, Type, \text{transaction}, M_7, h(L_{I-1}), h(O_{I+1}), O_I, Auth$$

$$D \rightarrow L: \quad L_I, MAC_{K_D}(L_I) \tag{8}$$

Audit Protocol

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$\begin{aligned} M_6 = \quad & N+1, \text{“}AUTH\text{”}, Len, D, h(O_{I+1}), h(L_{I-1}), \\ & \text{transaction}, Type, Auth, MAC_{K_D}(\text{transaction}) \end{aligned}$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

$$\begin{aligned} M_7 = \quad & MAC_{K_B}(N, I, \text{“}TACK\text{”}, Len, D, \text{transaction}, \\ & h(O_{I+1}), h(L_{I-1}), Type, Auth, MAC_{K_D}(\text{transaction})) \end{aligned}$$

$$B \rightarrow D: \quad \text{“}TACK\text{”}, Len, IV, \{M_7\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_7) \tag{7}$$

$$\begin{aligned} L_I = \quad & N, I, Len, Type, \text{transaction}, M_7, \\ & h(L_{I-1}), h(O_{I+1}), O_I, Auth \end{aligned}$$

$$D \rightarrow L: \quad L_I, MAC_{K_D}(L_I) \tag{8}$$

Audit Protocol

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$\begin{aligned} M_6 = \quad & N+1, \text{“}AUTH\text{”}, Len, D, h(O_{I+1}), h(L_{I-1}), \\ & \text{transaction}, Type, Auth, MAC_{K_D}(\text{transaction}) \end{aligned}$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

$$\begin{aligned} M_7 = \quad & MAC_{K_B}(N, I, \text{“}TACK\text{”}, Len, D, \text{transaction}, \\ & h(O_{I+1}), h(L_{I-1}), Type, Auth, MAC_{K_D}(\text{transaction})) \end{aligned}$$

$$B \rightarrow D: \quad \text{“}TACK\text{”}, Len, IV, \{M_7\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_7) \tag{7}$$

$$\begin{aligned} L_I = \quad & N, I, Len, Type, \text{transaction}, M_7, \\ & h(L_{I-1}), h(O_{I+1}), O_I, Auth \end{aligned}$$

$$D \rightarrow L: \quad L_I, MAC_{K_D}(L_I) \tag{8}$$

Audit Protocol

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$\begin{aligned} M_6 = \quad & N+1, \text{“}AUTH\text{”}, Len, D, h(O_{I+1}), h(L_{I-1}), \\ & \text{transaction}, Type, Auth, MAC_{K_D}(\text{transaction}) \end{aligned}$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

$$\begin{aligned} M_7 = \quad & MAC_{K_B}(N, I, \text{“}TACK\text{”}, Len, D, \text{transaction}, \\ & h(O_{I+1}), h(L_{I-1}), Type, Auth, MAC_{K_D}(\text{transaction})) \end{aligned}$$

$$B \rightarrow D: \quad \text{“}TACK\text{”}, Len, IV, \{M_7\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_7) \tag{7}$$

$$\begin{aligned} L_I = \quad & N, I, Len, Type, \text{transaction}, M_7, \\ & h(L_{I-1}), h(O_{I+1}), O_I, Auth \end{aligned}$$

$$D \rightarrow L: \quad L_I, MAC_{K_D}(L_I) \tag{8}$$

Audit Protocol

$$D \rightarrow U: \quad \text{transaction} \tag{4}$$

$$U \rightarrow D: \quad Auth \tag{5}$$

$$M_6 = \quad N+1, \text{“}AUTH\text{”}, Len, D, h(O_{I+1}), h(L_{I-1}), \text{transaction}, Type, Auth, MAC_{K_D}(\text{transaction})$$

$$D \rightarrow B: \quad \text{“}AUTH\text{”}, Len, IV, \{M_6\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_6) \tag{6}$$

$$M_7 = \quad MAC_{K_B}(N, I, \text{“}TACK\text{”}, Len, D, \text{transaction}, h(O_{I+1}), h(L_{I-1}), Type, Auth, MAC_{K_D}(\text{transaction}))$$

$$B \rightarrow D: \quad \text{“}TACK\text{”}, Len, IV, \{M_7\}_{E_{K_{BD1}}}, MAC_{K_{BD2}}(M_7) \tag{7}$$

$$L_I = \quad N, I, Len, Type, \text{transaction}, M_7, h(L_{I-1}), h(O_{I+1}), O_I, Auth$$

$$D \rightarrow L: \quad L_I, MAC_{K_D}(L_I) \tag{8}$$

Licence Attribution

- Original SecurID Image by Mateusz Adamowski `http://commons.wikimedia.org/wiki/User:Mateusza` licenced under Creative Commons Attribution ShareAlike 1.0 `http://creativecommons.org/licenses/by-sa/1.0/`. You are free to distribute my altered version under the same licence.