Szyfrowanie jako norma bezpieczeństwa 2016.

Mgr inż. Kamil Kaczyński
Wydział Cybernetyki
Wojskowa Akademia Techniczna

Zawirusowana armia 2.0

(…) Zawirusowanie komputerów używanych do sterowania bezzałogowymi samolotami to nie pierwsza tego typu wpadka armii USA. W 2008 roku zainfekowane zostały komputery Pentagonu, a wirus rozprzestrzenił się niemal po całej sieci amerykańskiego dowództwa. Usuwanie tamtej infekcji z poszczególnych maszyn... trwa do dziś. (…) Co prawda maszyny są odłączone od internetu, ale operatorom zezwolono na korzystanie z pendrive'ów (…)

Do innego incydentu związanego tym razem ***z bezzałogowymi samolotami doszło w 2009 roku.*** *Amerykańscy żołnierze* ***odkryli na laptopach irackich rebeliantów całe dni nagrań z kamer amerykańskich dron.*** *Okazało się, że* ***transmitowane do centrum dowodzenia obrazy nie były w żaden sposób szyfrowane.*** *Dzięki temu rebelianci mogli je przechwycić stosując oprogramowanie dostępne w internecie za... 26 dolarów*

Wp.pl, 10.10.2011

Wirus miał zatrzymać nuklearne zbrojenie.

*Izrael wypróbowywał wirusa komputerowego, który miał utrudnić Iranowi rozwój jego programu atomowego – poinformował w sobotę dziennik "New York Times". Gazeta pisze, że **Stuxnet został opracowany wspólnie przez specjalistów izraelskich i amerykańskich**.*

*(...) Irańskie wirówki miały mieć serię awarii w latach 2007 i 2008. W listopadzie ubiegłego roku prezydent Iranu Mahmud Ahmadineżad ujawnił, że **złośliwe oprogramowanie "spowodowało problemy" w niektórych irańskich wirówkach służących do wzbogacania uranu.** Twierdził jednak, że problemy te zostały rozwiązane.*

Anonimowi eksperci ds. bezpieczeństwa, na których powołuje się "New York Times", przypuszczają, że awarie mogły zostać spowodowane przez atak wirusa Stuxnet.

tvn24.pl, 16.01.2011.

Zakłady przemysłowe Iranu przedmiotem cyberataku.

Irańskie media poinformowały we wtorek o kolejnym cyberataku na sieci komputerowe Iranu z wykorzystaniem wirusa komputerowego Stuxnet. Tym razem jego celem były zakłady przemysłowe na południu kraju. Atak został odparty. (…)

*Władze w Teheranie zaostrzyły środki bezpieczeństwa sieci informatycznych w 2010 roku, po ataku wirusa komputerowego Stuxnet wykorzystanego do **destabilizacji prac irańskich instalacji nuklearnych**. Iran informował, że ataki wirusów Stuxnet oraz Flame stwierdzono też w sektorze naftowym, który **generuje ok. 80 proc. dochodów zagranicznych państwa.** (…)*

PAP, 25.12.2012

„Nie ma nic bardziej praktycznego niż dobra teoria matematyczna.”
Albert Einstein

Stuxnet zainfekował Rosjan.

Zainfekowana przez Stuxneta sieć komputerowa w Rosji, podobnie jak i ta w Iranie, była odcięta od Internetu. I podobnie jak w przypadku elektrowni w Natanz, Stuxnet dostał się do rosyjskiej infrastruktury poprzez podpięcie do komputera zainfekowanego nim wcześniej dysku USB. Miał w niej wyrządzić bliżej nieopisane szkody (przypomnijmy, że w Iranie niszczył wirówki do wzbogacania uranu).

Informacje odnośnie infekcji miał przekazać Kasperskiemu anonimowy pracownik jednej z elektrowni atomowych w Rosji. Kaspersky, który — przypomnijmy — jest powiązany z rosyjskimi służbami, zdecydował się ujawnić powyższe wiadomości podczas niedawnej konferencji prasowej w Australii. (…)

Niebezpiecznik.pl, 10.11.2013

Wyciek danych z Ambasady RP w Mińsku.

Przedstawiciele ruchu Anonymous opublikowali dzisiaj w nocy paczkę danych, które prawdopodobnie wyciekły z Ambasady RP na Białorusi. Ujawnione dane to skany paszportów i zaproszeń, wewnętrzna korespondencja urzędowa i dokumenty z logiem CBA.

Z oświadczenia włamywaczy wynika, że uzyskali oni dostęp do serwisu trade.gov.pl, czyli witryny Wydziałów Promocji Handlu i Inwestycji Ambasad i Konsulatów RP – zagranicznych placówek Ministerstwa Gospodarki, wspierających polski handel międzynarodowy. Serwis ten obsługuje także skrzynki poczty elektronicznej pracowników tychże wydziałów. Anonymous twierdzą, że mają dostęp do całej zawartości serwisu i dzisiaj zdecydowali się ujawnić jedynie dane pochodzące z placówki na Białorusi.

ZaufanaTrzeciaStrona.pl 16.10.2013

Wyciek danych z Ambasady RP w Mińsku.

From	To	Subject	Received	Created	Size
olga@prim	minsk@t	RUS: PRIME-TA	6 Oct 2013...	17 Sep 20...	765,316
minsk1@t	WPHI Mi	[Autoreply] FW:	6 Oct 2013...	17 Sep 20...	4,276
minsk1@t	WPHI Mi	[Autoreply] RE:	6 Oct 2013...	17 Sep 20...	27,524
minsk1@t	WPHI Mi	[Autoreply] FW:	6 Oct 2013...	17 Sep 20...	4,473
Amore Itali	undisclose		6 Oct 2013, ...	16 Sep 2013,...	316,927
olga@prim	minsk@t	RUS: PRIME-TA	6 Oct 2013...	17 Sep 20...	752,490
minsk1@tra	WPHI Min	[Autoreply] FW: w	6 Oct 2013, ...	16 Sep 2013,...	2,079,981
minsk1@t	WPHI Mi	[Autoreply] FW:	6 Oct 2013...	16 Sep 20...	171,651
minsk1@t	WPHI Mi	[Autoreply] FW:	6 Oct 2013...	16 Sep 20...	2,165,480
Aleksand	alger@t	współpraca przy	6 Oct 2013...	16 Sep 20...	2,078,767
Natalia D	minsk@t	SZ.P. Radca Wie	6 Oct 2013...	16 Sep 20...	162,277
WPHI Min	E.Hyjek	RE: Polska Grup	6 Oct 2013...	16 Sep 20...	88,699
Jolanta D	minsk@t	Prośba o poparc	6 Oct 2013...	16 Sep 20...	2,164,462
WPHI Min	minsk@t	FW: Polska Grup	6 Oct 2013...	16 Sep 20...	90,151
Zbigniew.	alger@t	Kostecki- skan p	6 Oct 2013...	16 Sep 20...	258,597
WPHI Mins	Anna.Z	WPHI w Minsku -	6 Oct 2013...	14 Sep 20....	62,142
WPHI Mins	'WPHI Min	PD: Baza danych p	6 Oct 2013, ...	14 Sep 2013,...	2,903,935
WPHI Mins	grodzki@	ODP: Polsko-Hiszp	6 Oct 2013, ...	14 Sep 2013,...	64,542
olga@prim	minsk@t	RUS: PRIME-TA	6 Oct 2013...	13 Sep 20...	808,051
Kubik Ane	undisclo	Firma Ekonaw z	6 Oct 2013...	13 Sep 20...	3,896,439
Elżbieta G	minsk@t	Prośba o pomoc	6 Oct 2013...	13 Sep 20...	1,542,980
Алексей П	minsk@tra	приглашения на	6 Oct 2013, ...	13 Sep 2013,...	211,756
olga@prime	minsk@tra	RUS: PRIME-TASS	6 Oct 2013, ...	12 Sep 2013,...	892,301

All | Unread | С фла...

From: WPHI Minsk-W.Pokladek <minsk1@trade.gov.pl>
To: 'WPHI Minsk' <minsk@trade.gov.pl>
Subject: PD: Baza danych polskich firm B2B

Za³¹cznik nr 3_Przewodn...
Za³¹cznik nr 2_Szczegó³o...
winmail.dat ~2.02 MB

przetestowanie od momentu otrzymania haseł ma wyłącznie 5 dni kalendarzowych.

Przetestowanie tej bazy na obecnym etapie ma na celu zapoznanie się przez Państwa z użytkowaniem nowej bazy, innej niż dotychczas funkcjonującej, oraz sprawdzenie przez Państwa czy zawartość bazy jest zgodna z treścią Szczegółowego Opisu Przedmiotu Zamówienia, który stanowi Załącznik nr 2 do niniejszego maila.

Aby sprawdzić bazę należy wpisać adres: https://mg.hbi.pl/ i zalogować się w panelu „DLA KLIENTÓW", wg podanego sposobu:

Użytkownik - przykład: ministerstwo_1
Hasło: 3gm

Każda placówka ma inną nazwę użytkownika i hasło. Indywidualne dane zawarte są w załączniku nr 1 do niniejszego maila.

W załączniku nr 3 do niniejszego mila przekazuję do Państwa wiadomości i wykorzystania „Przewodnik po bazie", przekazany nam przez Wykonawcę.

Po przetestowaniu bazy, uprzejmie proszę o pilne przesłanie, w terminie do dnia 16 września br., godz. 16.00 uzupełnionego Załącznika nr 1 (skanem) z uzupełnionymi zapisami w kolumnie „Uwagi/akceptacja" na adres: Malgorzata. @mg.gov.pl.

"DGP": Ambasada w Warszawie ma możliwości inwigilowania najważniejszych polskich instytucji.

Rosjanie mogą przechwytywać rozmowy telefoniczne przeprowadzane w promieniu kilometra od swojej ambasady. A w zasięgu znajdują się najważniejsze, polskie instytucje: MSZ, MON, CBA, Kancelaria Premiera czy Belweder – alarmują specjaliści i byli funkcjonariusze służb specjalnych.

Źródła związane z polskimi służbami specjalnymi potwierdzają, że Rosjanie są w stanie przechwytywać wszystkie rozmowy telefoniczne w odległości kilometra od ambasady – czytamy w "Dzienniku Gazecie Prawnej".

nieazlezna.pl 21.11.2013

Białoruś i Islandia przejmowały część ruchu Internetowego.

Renesys, firma zajmująca się analizą ruchu Internetowego na świecie, opublikowała interesującą analizę kilku incydentów bezpieczeństwa, które wydarzyły się w tym roku, a które dotyczyły przechwytywania routingu do 1500 adresów poprzez wstrzyknięcia prefiksów BGP. W sumie, przez ponad 60 dni obserwowano "na żywo" atak typu Man in the Middle — z tym, że "człowiekiem" w środku była Białoruś, a potem Islandia…

W lutym ruch Internetowy kilku firm i instytucji był przekierowywany przez Białoruś — a dokładniej, przez routery tamtejszego dostawcy Internetu "GlobalOneBel". Ataki trwały czasem po kilka minut, a czasem po kilka godzin. Ofiarami były w większości z instytucje finansowe, rządowe, a także lokalni dostawcy Internetu, z USA, Korei Płd., Niemiec, Czech oraz Litwy, Libii i Iranu.

Niebezpiecznik.pl 25.11.2013

Fałszywe certyfikaty SSL.

Od prawie 2 miesięcy irański rząd miał możliwość przechwytywania ruchu internetowego swoich obywateli. W tym celu wygenerowano fałszywe certyfikaty dla domen należących do m.in. Google, Mozilli i projektu TOR.

Fałszywy certyfikat Google używany przez Iran został wydany 11 lipca 2011 roku. Wystawcą jest holenderska firma DigiNotar. Niestety firma nie jest zbyt wylewna, jeśli chodzi o wyjaśnienia co i jak. Przyznała tylko, że 19 lipca odkryła włamanie do swojej sieci i usunęła nielegalnie wystawione certyfikaty. Okazuje się jednak, że pominęła ten googlowy… a może jeszcze jakiś? (…)

Niebezpiecznik.pl 04.09.2011

Francuski rząd podrobił certyfikat SSL Google.

Podlegający francuskiej agencji do spraw cyberbezpieczeństwa (ANSSI) urząd certyfikacyjny (CA) wygenerował fałszywe certyfikaty dla kilku domen Google. To pozwalało np. podsłuchiwać połączenie z GMailem, o ile połączenie ofiary przechodziło przez urządzenia na których wykorzystano ten certyfikat.

Google w swoim oświadczeniu ogranicza się do skąpego w detale komunikatu, że fałszywy certyfikat był wykorzystywany do "inspekcji szyfrowanego ruchu poprzez komercyjne urządzenie działające w prywatnej sieci i za zgodą jej użytkowników". Z lektury nieocenionego Reddita dowiemy się jednak, że winnym jest tak naprawdę francuskie Ministerstwo Finansów, któremu ANSSI przekazała klucz pośredniego CA (dzięki temu mogli generować "zaufane" certyfikaty dla dowolnych domen).

Niebezpiecznik.pl 09.12.2013

Two can keep a secret if one is dead.

Megamos Crypto złamane.

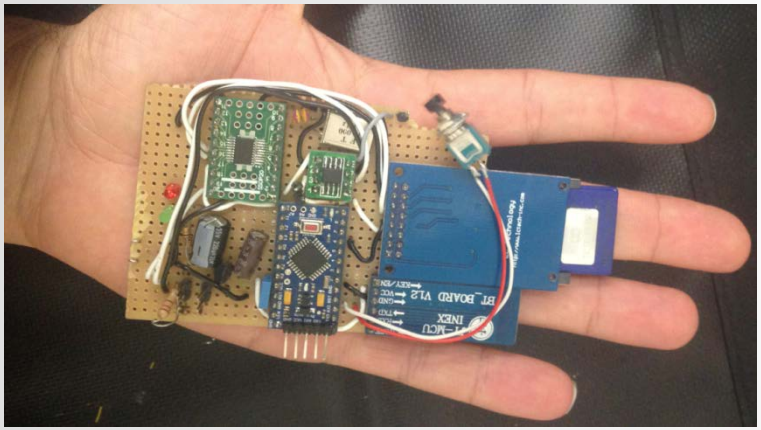
Megamos Crypto to system zabezpieczeń, stosowany w samochodach koncernu Volkswagen. Zabezpiecza jednak nie tylko popularne Seaty, Volkswageny czy Skody, ale także luksusowe Audi, Porsche, Bentleye i Lamborghini. Opracowany przez Volkswagena system kryptograficzny zabezpiecza transmisję między kluczykiem a immobilizerem, zapewniając, że tylko oryginalny kluczyk umożliwi otwarcie samochodu i odjechanie nim w siną dal. Choć na rynku oferowane są niezależne usługi kodowania/klonowania kluczyków, to sam algorytm nie był do tej pory uznawany za niebezpieczny.

ZaufanaTrzeciaStrona.pl 25.11.2013

There is no security on this earth. There is only opportunity.

General Douglas MacArthur

Bezprzewodowe hackowanie samochodów.



CHT to skrót od CAN Hacking Tools, niewielkiego urządzenia, które pozwala na przejęcie kontroli nad samochodowymi systemami zarządzania (np. hamulcami, zamkiem centralnym, światłami lub oknami).

Aby przejąć kontrolę nad samochodowym komputerem należy najpierw podpiąć CHT do ***CAN****(Controller Area Network), czyli samochodowej sieci komputerowej, do której podpina się wszystkie czujniki i kontrolery. Instalacja różni się w zależności od modelu samochodu: czasem trzeba będzie otworzyć maskę lub bagażnik (by dostać się do złącza OBD2), ale niekiedy wystarczy* ***po prostu wczołgać się pod samochód****. (…)*

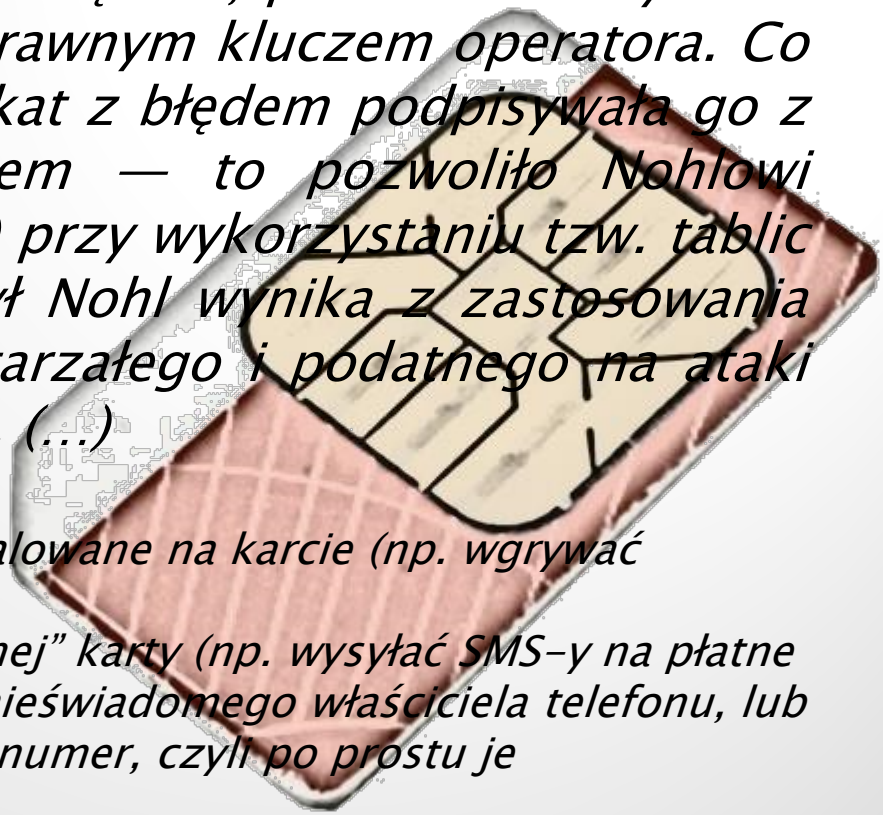
niebezpiecznik.pl 09.02.2014

Karty SIM podatne na ataki.

(…) wysyłając zgodnie z OTA komendy (SMS-y) do karty SIM, niektóre z nich będą odpowiadały błędem, ponieważ otrzymana komenda nie była podpisana poprawnym kluczem operatora. Co ciekawe, karta generując komunikat z błędem podpisywała go z kolei swoim unikatowym kluczem — to pozwoliło Nohlowi złamać klucz karty (w ok. minutę) przy wykorzystaniu tzw. tablic tęczowych. Problem, który odkrył Nohl wynika z zastosowania przez niektóre z kart SIM przestarzałego i podatnego na ataki szyfrowania 56-bitowym DES-em. (…)

Mając klucz karty SIM można:

- *kontrolować aplikacje operatora zainstalowane na karcie (np. wgrywać złośliwe aplety)*
- *wykonywać akcje w imieniu "zhackowanej" karty (np. wysyłać SMS-y na płatne numery, obciążając rachunek niczego nieświadomego właściciela telefonu, lub przekierowywać jego rozmowy na inny numer, czyli po prostu je podsłuchiwać)*
- *śledzić lokalizację właściciela karty. (…)*



Niebezpiecznik.pl 22.07.2013

IMSI Catcher

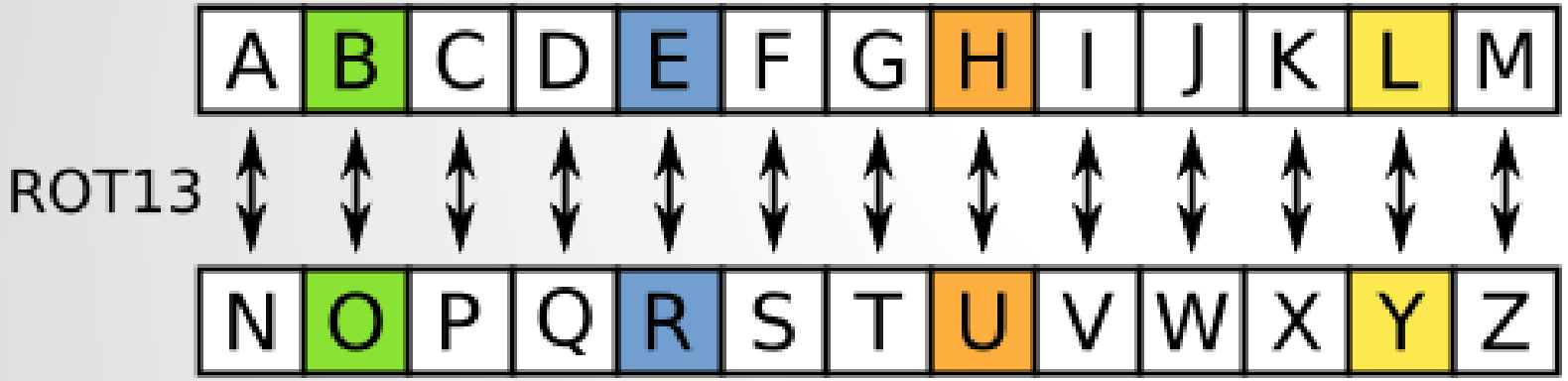
(...) Po włączeniu IMSI Catchera, telefony komórkowe w okolicy zauważają, że pojawił się mocniejszy sygnał sieci i przepinają się na fałszywy nadajnik. Fałszywy nadajnik z kolei łączy się z oryginalną siecią, aby przechwycone komórki mogły wykonywać i odbierać połączenia. Jest to klasyczny atak Man in the middle — będąc w środku komunikacji, fałszywy BTS wcale nie musi łamać szyfrowania protokołów sieci GSM, bo po prostu wymusza brak szyfrowania połączeń, korzystając z tego, iż większość telefonów komórkowych w żaden sposób nie sygnalizuje swojemu właścicielowi, że podłączyło się do sieci GSM bez szyfrowania.

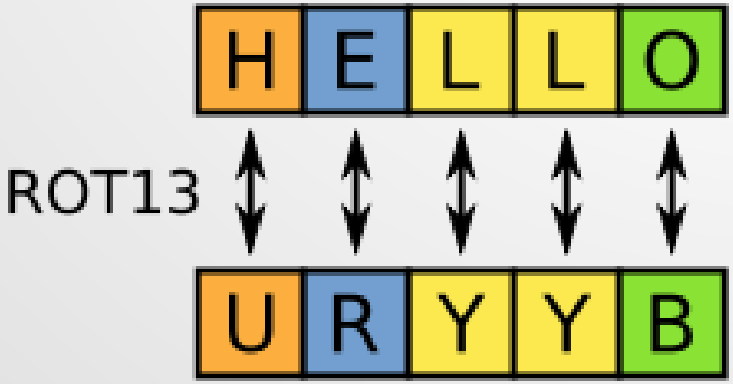
Brak szyfrowania pozwala fałszywemu BTS-owi na podsłuchiwanie rozmów, SMS-ów, transmisji pakietowej (Internet). Podsłuchiwane połączenia można oczywiście nagrywać. Dodatkowymi funkcjami fałszywego BTS-a jest korelacja danych, czyli możliwość namierzenia osoby, która zmieniła telefon (ale korzysta z tej samej karty) lub zmieniła kartę SIM (ale korzysta z tego samego telefonu) lub zmieniła kartę SIM i telefon jednocześnie (ale dalej wykonuje połączenia na te same numery).

niebezpiecznik.pl 26.10.2013

IMSI Catcher

Terroryści z Paryża





Terroryści z Paryża

Bezpieczeństwo danych w chmurze.

Wyciek wielu danych i informacji na temat nowego Wiedźmina

The download link for all the files is … And no it was not a „public" google drive leak, it was by hacking a developer named Dominika Gonsierowski and collecting files from her email and google drive that was shared by other members of CDProjekt. I am working on more games right now and will provide something soon. I have read all the requests in the other thread.

Reddit.com 22.06.2014

Wyciek danych z Ashley Madison

Włamanie do Plus Banku

W piątek przed północą na jednym z forów pojawiły się dane 500 klientów Plus Banku. Oprócz podstawowych danych takich jak imię i nazwisko właściciela lub nazwa firmy opublikowane zostały m.in. numery i daty ważności kart płatniczych, salda rachunków i historia transakcji. Co piątek haker będzie publikował kolejne dane, jeśli bank nie spełni jego żądań.

money.pl 13.06.2015

Jak żyć?

- Szyfrowanie asymetryczne
- Szyfrowanie symetryczne
- Schematy progowe
- Dedykowany hardware kryptograficzny
- Sprawdzone rozwiązania zamiast homebrew crypto
- Odpowiednie polityki bezpieczeństwa

The quieter you become, the more you are able to hear.

Ram Dass

PRISM

Dziękuję za uwagę

mgr inż. **Kamil Kaczyński**

Wydział Cybernetyki
Wojskowa Akademia Techniczna

What affected me most profoundly was the realization that the sciences of cryptography and mathematics are very elegant, pure sciences. I found that the ends for which these pure sciences are used are less elegant.
James Sanborn